PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-175605
(43)Date of publication of application : 29.06.2001

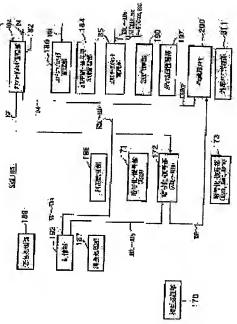
(51)Int.Cl. G06F 15/00
G10L 11/00
H04H 1/00
H04L 9/10
H04N 7/167
H04N 7/173

(21)Application number : 11-359896
(22)Date of filing : 17.12.1999

(71)Applicant : SONY CORP
(72)Inventor : NONAKA SATOSHI
EZAKI TADASHI

(54) DATA PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data processor which can effectively protect the profit of a provider of content data.
SOLUTION: Secure container 104 containing content data ciphered by using content key data, the mentioned ciphered content key data, and title deed data showing the handling of the content data is inputted from a content provider management part 180, and a charging process part 187 determines at least one of the purchase style and use style of the content data according to the handling that the title deed data indicate. The charging process part 187 generates history data showing the result of the mentioned decision. Each process part is stored in a tamper-resisting circuit module.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－175605
（Ｐ2001－175605Ａ）
(43)公開日　平成13年６月29日(2001.6.29)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｚ	５Ｂ０８５
Ｇ１０Ｌ　11/00		Ｈ０４Ｈ　1/00	Ｆ	５Ｃ０６４
Ｈ０４Ｈ　1/00		Ｈ０４Ｎ　7/173	６４０Ａ	５Ｊ１０４
Ｈ０４Ｌ　9/10		Ｇ１０Ｌ　9/00	Ｅ	９Ａ００１
Ｈ０４Ｎ　7/167		Ｈ０４Ｌ　9/00	６２１Ａ	

審査請求　未請求　請求項の数65　ＯＬ　（全119頁）　最終頁に続く

(21)出願番号　特願平11－358896

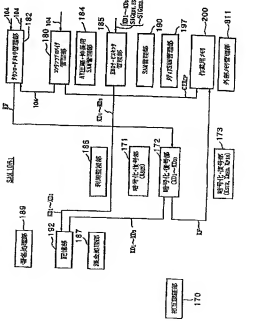
(22)出願日　平成11年12月17日(1999.12.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　野中　聡
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　江崎　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　データ処理装置

(57)【要約】
【課題】　コンテンツデータの提供者の利益を効果的に保護できるデータ処理装置を提供する。
【解決手段】　コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したセキュアコンテナ１０４をコンテンツプロバイダ管理部１８０から入力し、課金処理部１８７において、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。課金処理部１８７において、前記決定の結果を示す履歴データを生成する。各処理部は、耐タンパ性の回路モジュール内に格納されている。



1

【特許請求の範囲】

【請求項１】コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項２】前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項１に記載のデータ処理装置。

【請求項３】前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する請求項２に記載のデータ処理装置。

【請求項４】前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する請求項２に記載のデータ処理装置。

【請求項５】前記記録媒体がセキュアＲＡＭ領域を有する場合に、前記権利書データおよび前記暗号化された前記利用制御データを前記セキュアＲＡＭ領域に記録するように制御する記録制御手段を前記耐タンパ性の回路モジュール内にさらに有する請求項４に記載のデータ処理装置。

【請求項６】前記記録媒体が相互認証機能を持つ耐タンパ性のデータ処理装置を有する場合に、前記権利書データおよび前記暗号化された前記利用制御データを前記記録媒体の前記データ処理装置に記録するように制御する記録制御手段を前記耐タンパ性の回路モジュール内にさらに有する請求項４に記載のデータ処理装置。

【請求項７】前記履歴データ生成手段は、

前記コンテンツデータを提供したデータ提供装置の識別子、ユーザの識別子、

当該データ処理装置の識別子、当該コンテンツデータに係わるライセンス所有者の識別子を少なくとも記述した前記履歴データを生成する請求項１に記載のデータ処理装置。

2

【請求項８】前記利用制御データ生成手段は、

前記購入形態を決定したユーザの識別子および前記決定された購入形態を少なくとも記述した前記利用制御データを生成する請求項２に記載のデータ処理装置。

【請求項９】前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらに行い、

前記データ処理装置は、

前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項１に記載のデータ処理装置。

【請求項１０】前記署名データは、前記コンテンツ鍵データおよび前記権利書データの作成者の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記作成者の公開鍵データを用いて前記署名データの正当性を検証する請求項９に記載のデータ処理装置。

【請求項１１】前記署名データは、前記コンテンツ鍵データおよび前記権利書データの送り元の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記送り元の公開鍵データを用いて前記署名データの正当性を検証する請求項９に記載のデータ処理装置。

【請求項１２】前記入力処理手段は、前記コンテンツデータの署名データを入力する処理をさらに行い、

前記データ処理装置は、

前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項１に記載のデータ処理装置。

【請求項１３】前記入力処理手段は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて秘密鍵データを用いて作成された署名データと、前記秘密鍵データに対応する公開鍵データとを入力する処理をさらに行い、

前記データ処理装置は、

前記公開鍵データを用いて、前記署名データの正当性を検証する署名処理手段を前記耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う請求項１に記載のデータ処理装置。

【請求項１４】前記コンテンツ鍵データは、ライセンス鍵データを用いて暗号化されており、前記データ処理装置は、

前記ライセンス鍵データを記憶する記憶手段をさらに有し、

前記復号手段は、前記記憶手段から読み出した前記ライセンス鍵データを用いて前記コンテンツ鍵データを復号する請求項１に記載のデータ処理装置。

【請求項１５】前記データ処理装置は、他の装置との間で、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一のデータをオンラインで送受信する場合に、前記他の装置との間で相互認証を行う相互認証手段と、

前記相互認証によって得られたセッション鍵データを用いて、前記送受信を行うデータの暗号化および復号を行う暗号化・復号手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項１に記載のデータ処理装置。

【請求項１６】前記データ処理装置は、他の装置との間でデータの送受信を行う際に、無効にされた装置のリストを記述したリボケーションリストを参照し、当該リボケーションリストに前記他の装置が無効であることが示されていない場合に、前記他の装置との間でデータの送受信を行う請求項１５に記載のデータ処理装置。

【請求項１７】コンテンツデータの提供をデータ提供装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記履歴データを前記管理装置に出力する出力手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項１８】前記入力処理手段は、

前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う請求項１７に記載のデータ処理装置。

【請求項１９】前記入力処理手段は、

前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データを格納したキーファイルとを入力する処理を行う請求項１８に記載のデータ処理装置。

【請求項２０】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項１９に記載のデータ処理装置。

【請求項２１】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段と前記耐タンパ性の回路モジュール内にさらに有する請求項２０に記載のデータ処理装置。

【請求項２２】前記入力処理手段は、

前記コンテンツファイルの作成者および送り主である前記データ提供装置の第１の署名データと、前記キーファイルの作成者である前記管理装置の第２の署名データと、前記キーファイルの送り主である前記データ提供装置の第３の署名データとをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記第１の署名データ、前記第２の署名データおよび前記第３の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記第１の署名データ、前記第２の署名データおよび前記第３の署名データの正当性が確認された後に、前記決定を行う請求項１９に記載のデータ処理装置。

【請求項２３】前記第１の署名データおよび前記第３の署名データは、前記データ提供装置の秘密鍵データを用いて作成されており、

前記第２の署名データは、前記管理装置の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記データ提供装置の公開鍵データを用いて前記第１の署名データおよび前記第３の署名データの検証を行い、前記管理装置の公開鍵データを用

いて前記第２の署名データの検証を行う請求項２２に記載のデータ処理装置。

【請求項２４】前記入力処理手段は、前記データ提供装置の秘密鍵データに対応する公開鍵データをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記署名処理手段は、前記モジュールに格納された公開鍵データを用いて、前記第１の署名データおよび前記第３の署名データの検証を行う請求項２３に記載のデータ処理装置。

【請求項２５】前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールの入力処理を行い、

前記データ処理装置は、

前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する請求項１８に記載のデータ処理装置。

【請求項２６】コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項２７】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツデータの購入形態の決定処理が行われる

際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項２８】前記入力処理手段は、

前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う請求項２７に記載のデータ処理装置。

【請求項２９】前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データ格納したキーファイルと、前記価格データとを入力する処理を行う請求項２８に記載のデータ処理装置。

【請求項３０】前記購入形態が決定されたときに、当該決定された購入形態を示す利用制御データを生成する利用制御データ生成手段と、

前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と、

前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段と、

前記コンテンツファイル、前記キーファイルおよび前記暗号化された利用制御データを前記記録媒体に記録するように制御する記録制御手段とを前記耐タンパ性の回路モジュール内にさらに有する請求項２９に記載のデータ処理装置。

【請求項３１】前記入力処理手段は、

前記コンテンツファイルの作成者および送り主である前記データ提供装置の第１の署名データと、前記コンテンツファイルの送り主である前記データ配給装置の第２の署名データと、前記キーファイルの作成者である前記管理装置の第３の署名データと、前記キーファイルの送り主である前記データ提供装置の第４の署名データと、前記キーファイルの送り主である前記データ配給装置の第５の署名データと、前記価格データの作成者および送り主である前記データ配給装置の第６の署名データをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記第１の署名データ、前記第２の署名データ、前記第３の署名データ、前記第４の署名データ、前記第５の署名データおよび前記第６の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、

前記決定手段は、前記署名処理手段によって前記第１の署名データ、前記第２の署名データ、前記第３の署名データ、前記第４の署名データ、前記第５の署名データおよび第６の署名データの正当性が確認された後に、前記

決定を行う請求項２８に記載のデータ処理装置。

【請求項３２】前記第１の署名データおよび前記第４の署名データは、前記データ提供装置の秘密鍵データを用いて作成されており、

前記第２の署名データ、前記第５の署名データおよび前記第６の署名データは、前記データ配給装置の秘密鍵データを用いて作成されており、

前記第３の署名データは、前記管理装置の秘密鍵データを用いて作成されており、

前記署名処理手段は、前記データ提供装置の公開鍵データを用いて前記第１の署名データおよび前記第４の署名データの検証を行い、前記データ配給装置の公開鍵データを用いて前記第２の署名データ、前記第５の署名データおよび前記第６の署名データの検証を行い、前記管理装置の公開鍵データを用いて前記第３の署名データの検証を行う請求項３１に記載のデータ処理装置。

【請求項３３】前記入力処理手段は、前記データ提供装置の秘密鍵データに対応する公開鍵データと、前記データ配給装置の秘密鍵データに対応する公開鍵データとをさらに格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記署名処理手段は、前記モジュールに格納された前記データ提供装置の公開鍵データを用いて前記第１の署名データおよび前記第４の署名データの検証を行い、前記モジュールに格納された前記データ配給装置の公開鍵データを用いて前記第２の署名データ、前記第５の署名データおよび前記第６の署名データの検証を行う請求項３２に記載のデータ処理装置。

【請求項３４】前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールを入力する処理を行い、

前記データ処理装置は、

前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する請求項２８に記載のデータ処理装置。

【請求項３５】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力するとともに、前記履歴データを前記管理装置に出力する出力手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項３６】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理装置において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第１の処理モジュールと、

前記受信したモジュールに格納された前記権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納された前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力するとともに前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを有するタンパ性の第２の処理モジュールとを有するデータ処理装置。

【請求項３７】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、

当該データ処理装置の秘密鍵データを記憶する記憶回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場

9

合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項３８】前記前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路をさらに有し、

前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う請求項３７に記載のデータ処理装置。

【請求項３９】前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路とをさらに有する請求項３７に記載のデータ処理装置。

【請求項４０】前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する請求項３７に記載のデータ処理装置。

【請求項４１】記録媒体に搭載された相互認証機能を持つデータ処理回路、半導体記憶回路およびＩＣカードの少なくとも一つとの間で通信を行うインターフェイスをさらに有する請求項３７に記載のデータ処理装置。

【請求項４２】有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、

前記記憶回路は、前記ライセンス鍵データを記憶し、

前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、

前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、

前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する請求項３７に記載のデータ処理装置。

【請求項４３】前記公開鍵暗号回路、前記共通鍵暗号回路および前記ハッシュ関数回路のうち少なくとも一の回

10

路を、前記記憶回路に記憶されたプログラムを前記演算処理回路で実行して実現する請求項３７に記載のデータ処理装置。

【請求項４４】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、

当該データ処理装置の秘密鍵データを記憶する記憶回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、を有する耐タンパ性の回路モジュールと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項４５】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項４６】前記記憶回路は、前記記録領域に記録されるコンテンツデータがコンテンツ鍵データを用いて暗号化されている場合に、暗号化された前記コンテンツ鍵データを記憶する請求項４５に記載のデータ処理装置。

【請求項４７】前記記憶回路は、前記記録領域に記録されるコンテンツデータの取り扱いを示す権利書データを記憶する請求項４６に記載のデータ処理装置。

【請求項４８】前記記憶回路は、他の装置と通信を行う際に当該装置の有効性を判断する情報を示すリボケーションリストを記憶し、

前記演算処理回路は、前記リボケーションリストに基づいて、前記他の装置が無効であると判断した場合に、前記他の装置との間の通信を停止する請求項４５に記載のデータ処理装置。

【請求項４９】前記記録媒体の記録領域がＲＯＭ型であり、当該記録領域にコンテンツ鍵データで暗号化されたコンテンツデータが記録されている場合に、

前記記憶回路は、初期状態で、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを記憶している請求項４５に記載のデータ処理装置。

【請求項５０】前記記録媒体の記録領域がＲＡＭ型である場合に、

前記記憶回路は、前記記録領域にコンテンツ鍵データで暗号化されたコンテンツデータが記録される際に、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを記憶する請求項４５に記載のデータ処理装置。

【請求項５１】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項５２】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項５３】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

外部インターフェイスと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項５４】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、

当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

外部インターフェイスと、

演算処理回路と、

前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の

回路モジュール内に有するデータ処理装置。

【請求項５５】ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、

他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、

外部インターフェイスとを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路の制御を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項５６】コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、

他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、

前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項５７】前記データの伸長が部分的に行われるように制御する半開示制御回路をさらに有する請求項５６に記載のデータ処理装置。

【請求項５８】前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路をさらに有する請求項５６に記載のデータ処理装置。

【請求項５９】コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、

他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツデータに対応して入力したソフトウェアに基づいて、前記コンテンツデータの圧縮および伸長の少なくとも一方と、前記圧縮および伸長の対象となるコンテンツデータに対して電子透かし情報の検出および埋め込みを行う演算処理回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項６０】ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項６１】前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路をさらに有する請求項６０に記載のデータ処理装置。

【請求項６２】前記データ処理装置の識別子を記憶する記憶回路と、

前記データ処理装置の識別子および前記記録媒体の識別子に基づいて前記記録媒体にユニークな記録用鍵データを生成する記録用鍵データ生成回路とをさらに有し、

前記共通鍵暗号回路は、前記記録用鍵データを用いて、前記記録媒体に記録されるコンテンツデータの暗号化および復号を行う請求項６１に記載のデータ処理装置。

【請求項６３】ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項６４】ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用

いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【請求項６５】ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置において、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、

前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有するデータ処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、提供されたコンテンツデータに関連する処理を行うデータ処理装置に関する。

【０００２】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このようなデータ提供システムの一つに、音楽データを配信する従来のＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムがある。

【０００３】図１０９は、従来のＥＭＤシステム７００の構成図である。図１０９に示すＥＭＤシステム７００では、コンテンツプロバイダ７０１ａ，７０１ｂが、サービスプロバイダ７１０に対し、コンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報７０５ａ，７０５ｂ，７０５ｃには、例えば、ＳＣＭＳ(Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ７１０の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【０００４】サービスプロバイダ７１０は、受信したコンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとをセッション鍵データを用いて復号する。そして、サービスプロバイダ７１０は、復号したあるいはオフラインで受け取ったコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに、著作権情報７０５ａ，７０５ｂ，７０５ｃを埋め込んで、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを生成する。このとき、サービスプロバイダ７１０は、例えば、著作権情報７０５ａ，７０５ｂ，７０５ｃのうち電子透かし情報をコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにＳＣＭＳ情報を埋め込む。さらに、サービスプロバイダ７１０は、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、鍵データベース７０６から読み出したコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いてそれぞれ暗号化する。その後、サービスプロバイダ７１０は、暗号化されたコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを格納したセキュアコンテナ７２２を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置７０９に存在するＣＡ(Conditional Access)モジュール７１１に送信する。

【０００５】ＣＡモジュール７１１は、セキュアコンテナ７２２をセッション鍵データを用いて復号する。また、ＣＡモジュール７１１は、電子決済やＣＡなどの課金機能を用いて、サービスプロバイダ７１０の鍵データベース７０６からコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置７０９において、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、それぞれコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号することが可能になる。このとき、ＣＡモジュール７１１は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報７２１を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ７１０の権利処理モジュール７２０に送信する。この場合に、ＣＡモジュール７１１は、サービスプロバイダ７１０が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

【０００６】サービスプロバイダ７１０は、ＣＡモジュール７１１から課金情報７２１を受信すると、サービス

プロバイダ７１０とコンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃとの間で利益配分を行う。このとき、サービスプロバイダ７１０から、コンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃへの利益配分は、例えば、ＪＡＳＲＡＣ(Japanese Societyfor Rights of Authors, Composers and Publishers:日本音楽著作権協会）を介して行われる。また、ＪＡＳＲＡＣによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【０００７】また、端末装置７０９では、コンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号したコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、ＲＡＭ型の記録媒体７２３などに記録する際に、著作権情報７０５ａ，７０５ｂ，７０５ｃのＳＣＭＳビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃに埋め込まれたＳＣＭＳビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【０００８】

【発明が解決しようとする課題】ところで、ＳＣＭＳは、コンテンツデータを例えば２世代以上のわたって複製することを禁止するものであり、１世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【０００９】また、上述したＥＭＤシステム７００では、サービスプロバイダ７１０が暗号化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ７０１の関係者はサービスプロバイダ７１０の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ７０１の利益が不当に損なわれる可能性が高いという問題がある。また、上述したＥＭＤシステム７００では、ユーザの端末装置７０９がサービスプロバイダ７１０から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ７０１の利益が不当に損なわれるという問題がある。

【００１０】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護することを可能にするデータ処理装置を提供することを目的とする。また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ処理装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第１の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された

前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００１２】本発明の第１の観点のデータ処理装置の作用を以下に示す。例えば、コンテンツデータを提供するデータ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとが、入力手段に入力される。次に、決定手段によって、ユーザによるコンテンツデータの購入形態および利用形態を決定する操作に応じて、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。すなわち、ユーザによるコンテンツデータの決定は、権利書データが示すコンテンツデータの取り扱いに従って行われる。この場合に、データ提供装置の関係者が権利書データを作成することで、当該関係者がコンテンツデータの購入および利用を制御できる。次に、履歴データ生成手段によって、前記決定の結果を示す履歴データが生成される。当該履歴データは、例えば、コンテンツデータの利用等に伴って得られた利益を関係者に分配する管理装置に送られる。また、当該第１の観点のデータ処理装置では、復号手段によって、前記コンテンツ鍵データを復号が行われる。すなわち、耐タンパ性の回路モジュール内で、コンテンツ鍵データの復号を行うことで、所定の購入形態の決定処理を経た後にのみ、コンテンツ鍵データを用いたコンテンツデータの復号を可能にすることができ、コンテンツデータの不正使用を効果的に阻止できる。

【００１３】また、本発明の第１の観点のデータ処理装置は、好ましくは、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段とを前記耐タンパ性の回路モジュール内にさらに有する。

【００１４】また、本発明の第１の観点のデータ処理装置は、好ましくは、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記コンテンツデータを前記記録媒体に記録する際に用いられる記録装置に対応した記録用鍵データと、前記記録媒体に対応したメディア鍵データとを用いて暗号化する暗号化手段を前記耐タンパ性の回路モジュール内にさらに有する。

【００１５】また、本発明の第１の観点のデータ処理装

置は、好ましくは、前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらに行い、前記データ処理装置は、前記署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う。

【００１６】また、本発明の第１の観点のデータ処理装置は、好ましくは、前記データ処理装置は、他の装置との間でデータの送受信を行う際に、無効にされた装置のリストを記述したリポケーションリストを参照し、当該リポケーションリストに前記他の装置が無効であることが示されていない場合に、前記他の装置との間でデータの送受信を行う。

【００１７】また、本発明の第２の観点のデータ処理装置は、コンテンツデータの提供をデータ提供装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００１８】本発明の第２の観点のデータ処理装置の作用を説明する。入力処理手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データを入力する処理が行われる。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。次に、出力手段において、前記履歴データが前記管理装置に出力される。

【００１９】また、本発明の第２の観点のデータ処理装置は、好ましくは、前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う。

【００２０】また、本発明の第２の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データを格納したキーファイルとを入力する処理を行う。

【００２１】また、本発明の第２の観点のデータ処理装置は、好ましくは、前記コンテンツデータが圧縮されたデータである場合に、前記圧縮されたコンテンツデータを伸長するための伸長用ソフトウェアをさらに格納した前記コンテンツファイルを格納した前記モジュールの入力処理を行い、前記データ処理装置は、前記伸長用ソフトウェアを用いて、前記コンテンツデータが伸長されるように制御する制御手段をさらに有する。

【００２２】また、本発明の第３の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００２３】本発明の第３の観点のデータ処理装置の作用を説明する。入力処理手段において、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したモジュールが所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力される。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、復号手段において、前記コンテンツ鍵データが復号される。

【００２４】また、本発明の第４の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記

決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００２５】本発明の第４の観点のデータ処理装置の作用を説明する。入力手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを入力する処理が行われる。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、出力手段によって、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データが出力される。また、出力手段によって、前記履歴データが前記管理装置に出力される。また、復号手段において、前記コンテンツ鍵データが復号される。

【００２６】また、本発明の第４の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツファイルおよび前記キーファイルを格納したモジュールを入力する処理を行う。

【００２７】また、本発明の第４の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツデータを格納したコンテンツファイルと、前記コンテンツ鍵データおよび前記権利書データ格納したキーファイルと、前記価格データとを入力する処理を行う。

【００２８】また、本発明の第５の観点のデータ処理装置は、好ましくは、前記入力処理手段は、前記コンテンツファイルの作成者および送り主である前記データ提供装置の第１の署名データと、前記コンテンツファイルの送り主である前記データ配給装置の第２の署名データと、前記キーファイルの作成者である前記管理装置の第３の署名データと、前記キーファイルの送り主である前記データ提供装置の第４の署名データと、前記キーファイルの送り主である前記データ配給装置の第５の署名データと、前記価格データの作成者および送り主である前記データ配給装置の第６の署名データをさらに格納した前記モジュールを入力する処理を行い、前記データ処理装置は、前記第１の署名データ、前記第２の署名データ、前記第３の署名データ、前記第４の署名データ、前記第５の署名データおよび前記第６の署名データの正当性を検証する署名処理手段を耐タンパ性の回路モジュール内にさらに有し、前記決定手段は、前記署名処理手段によって前記第１の署名データ、前記第２の署名データ、前記第３の署名データ、前記第４の署名データ、前記第５の署名データおよび前記第６の署名データの正当性が確認された後に、前記決定を行う。

【００２９】また、本発明の第６の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、前記コンテンツデータの購入および利用の少なくとも一方に応じて得られた利益を所定の権利者に分配するための利益分配処理を行う管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力する処理を行う入力処理手段と、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に、前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００３０】本発明の第６の観点のデータ処理装置の作用を説明する。入力処理手段において、データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体を介して入力される。次に、決定手段において、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方が決定される。次に、履歴データ生成手段において、前記決定の結果を示す履歴データが生成される。また、出力手段において、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データが出力されると共に、前記履歴データが前記管理装置に出力される。また、復号手段において、前記コンテンツ鍵データが復号される。

【００３１】また、本発明の第７の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについ

て付けた価格データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第１の処理モジュールを有する。また、当該第７の観点のデータ処理装置は、前記受信したモジュールに格納された前記権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納された前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを有する耐タンパ性の第２の回路モジュールを有する。

【００３２】本発明の第８の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを前記媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有する。

【００３３】また、本発明の第８の観点のデータ処理装置は、好ましくは、前記前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路をさらに有し、前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う。

【００３４】また、本発明の第８の観点のデータ処理装置は、好ましくは、前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路とをさらに有する。

【００３５】また、本発明の第８の観点のデータ処理装置は、好ましくは、前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する。

【００３６】また、本発明の第８の観点のデータ処理装置は、好ましくは、有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する。

【００３７】また、本発明の第８の観点のデータ処理装置は、好ましくは、前記公開鍵暗号回路、前記共通鍵暗号回路および前記ハッシュ関数回路のうち少なくとも一の回路を、前記記憶回路に記憶されたプログラムを前記演算処理回路で実行して実現する。

【００３８】また、本発明の第９の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認

証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスとを有する耐タンパ性の回路モジュールと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【００３９】また、本発明の第１０の観点のデータ処理装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【００４０】また、本発明の第１０の観点のデータ処理装置は、好ましくは、前記記憶回路は、前記記録領域に記録されるコンテンツデータがコンテンツ鍵データを用いて暗号化されている場合に、暗号化された前記コンテンツ鍵データを記憶する。

【００４１】また、本発明の第１０の観点のデータ処理装置は、好ましくは、前記記憶回路は、他の装置と通信を行う際に当該装置の有効性を判断する情報を示すリボケーションリストを記憶し、前記演算処理回路は、前記リボケーションリストに基づいて、前記他の装置が無効であると判断した場合に、前記他の装置との間の通信を停止する。

【００４２】また、本発明の第１１の観点のデータ処理装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスと、演算処理回路と、前記記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【００４３】また、本発明の第１２の観点のデータ処理装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【００４４】また、本発明の第１３の観点のデータ処理装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置との間で相互認証を行い、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスとを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【００４５】また、本発明の第１４の観点のデータ処理装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、外部インターフェイスと、演算処理回路と、前記記憶回路に対してのアクセスを、演算処理回路からの命令に応じて行う記憶回路制御回路とを耐タンパ性の回路モジュール内に有する。

【００４６】また、本発明の第１５の観点のデータ処理

装置は、ＲＯＭ型あるいはＲＡＭ型の記録領域を持つ記録媒体に搭載されるデータ処理装置であって、当該データ処理装置の秘密鍵データと、前記記録領域に記憶されるデータを暗号化する際に用いる鍵データを記憶する記憶回路と、他の装置が秘密鍵データを用いて作成した署名データを対応する公開鍵データを用いて検証し、前記秘密鍵データを用いて署名データを作成する公開鍵暗号回路と、外部インターフェイスと、を有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路の制御を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【００４７】また、本発明の第１６の観点のデータ処理装置は、コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有する。

【００４８】また、本発明の第１６の観点のデータ処理装置は、好ましくは、前記データの伸長が部分的に行われるように制御する半開示制御回路をさらに有する。

【００４９】また、本発明の第１７の観点のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。

【００５０】また、本発明の第１７の観点のデータ処理装置は、好ましくは、前記データ処理装置の識別子を記憶する記憶回路と、前記データ処理装置の識別子および前記記録媒体の識別子に基づいて前記記録媒体にユニークな記録用鍵データを生成する記録用鍵データ生成回路とをさらに有し、前記共通鍵暗号回路は、前記記録用鍵データを用いて、前記記録媒体に記録されるコンテンツデータの暗号化および復号を行う。

【００５１】また、本発明の第１８の観点のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。

【００５２】また、本発明の第１９の観点のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【００５３】また、本発明の第２０の観点のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを公開鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記公開鍵データを用いて署名データを作成する公開鍵暗号回路と、前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを有する耐タンパ性の回路モジュールと、前記回路モジュール内の回路を制御する処理を耐タンパ性のプログラムに基づいて実行する演算処理回路とを有する。

【００５４】

【発明の実施の形態】以下、本発明の実施形態に係わるＥＭＤ（Electronic Music Distribution：電子音楽配信）システムについて説明する。

第１実施形態

図１は、本実施形態のＥＭＤシステム１００の構成図で

ある。本実施形態において、ユーザに配信されるコンテンツ(Content)データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図１に示すように、EMDシステム１００は、コンテンツプロバイダ１０１、EMDサービスセンタ（クリアリング・ハウス、以下、ＥＳＣとも記す）１０２およびユーザホームネットワーク１０３を有する。ここで、コンテンツプロバイダ１０１、EMDサービスセンタ１０２およびＳＡＭ１０５$_1$～１０５$_4$が、本発明のデータ提供装置、管理装置およびデータ処理装置にそれぞれ対応している。先ず、EMDシステム１００の概要について説明する。EMDシステム１００では、コンテンツプロバイダ１０１は、自らが提供しようとするコンテンツのコンテンツデータＣを暗号化する際に用いたコンテンツ鍵データＫｃ、コンテンツデータＣの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ１０６、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある複数機関であるEMDサービスセンタ１０２に送る。

【００５５】EMDサービスセンタ１０２は、コンテンツプロバイダ１０１から受けたコンテンツ鍵データＫｃ、権利書データ１０６並びに電子透かし情報鍵データを登録（認証および複成化）する。また、EMDサービスセンタ１０２は、対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_5$を暗号化したコンテンツ鍵データＫｃ、権利書データ１０６および自らの署名データなどを格納したキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送る。ここで、当該署名データは、キーファイルＫＦの改竄の有無、キーファイルＫＦの作成者の正当性およびキーファイルＫＦがEMDサービスセンタ１０２において正規に登録されたことを検証するために用いられる。

【００５６】また、コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成し、当該生成したコンテンツファイルＣＦと、EMDサービスセンタ１０２から受けたキーファイルＫＦと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）１０４を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク１０３に配給する。ここで、セキュアコンテンツ１０４内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【００５７】ユーザホームネットワーク１０３は、例えば、ネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$を有する。ネットワーク機器１６０$_1$は、ＳＡＭ(Secure Application Module) １０５$_1$を内蔵している。ＡＶ機器１６０$_2$～１６０$_4$は、それぞれＳＡＭ

１０５$_2$～１０５$_4$を内蔵している。ＳＡＭ１０５$_1$～１０５$_4$相互間は、例えば、ＩＥＥＥ(Institute ofElectrical and Electronics Engineers) １３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

【００５８】ＳＡＭ１０５$_1$～１０５$_4$は、ネットワーク機器１６０$_1$がコンテンツプロバイダ１０１からネットワークなどを介してオンラインで受信したセキュアコンテナ１０４、および／または、コンテンツプロバイダ１０１からＡＶ機器１６０$_2$～１６０$_4$に記録媒体を介してオフラインで供給されたセキュアコンテナ１０４を対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_5$を用いて復号した後に、署名データの検証を行う。ＳＡＭ１０５$_1$～１０５$_4$に供給されたセキュアコンテナ１０４は、ネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ１０５$_1$～１０５$_4$は、上述したセキュアコンテナ１０４の購入・利用の履歴を利用履歴(Usage Log) データ１０８として記録するとともに、購入形態を示す利用制御データ１６６を作成する。利用履歴データ１０８は、例えば、EMDサービスセンタ１０２からの要求に応じて、ユーザホームネットワーク１０３からEMDサービスセンタ１０２に送信される。利用制御データ１６６は、例えば、購入形態が決定される度に、ユーザホームネットワーク１０３からEMDサービスセンタ１０２に送信される。

【００５９】EMDサービスセンタ１０２は、利用履歴データ１０８に基づいて、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが決済機関９１に支払った金銭が、EMDサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１に支払われる。また、EMDサービスセンタ１０２は、一定期間毎に、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【００６０】本実施形態では、EMDサービスセンタ１０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、EMDサービスセンタ１０２は、中立の立場にある最高の権威機関であるルート認証局９２に対しての（ルート認証局９２の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ１０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ１０２は、コンテンツプロバイダ１０１の権

利書データ１０６を登録して権威化することも、ＥＭＤサービスセンタ１０２の認証機能の一つである。また、ＥＭＤサービスセンタ１０２は、例えば、ライセンス鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ１０２は、権威化した権利書データ１０６に記述された標準小売価格ＳＲＰ（Suggested Retailer' Price）と$SAM_1$０５ｉ～$SAM_1$０５ｉから入力した利用履歴データ１０８とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ１０１に分配する権利処理（利益分配）機能を有する。

【００６１】図２は、セキュアコンテナ１０４の概念をまとめた図である。図２に示すように、セキュアコンテナ１０４には、コンテンツプロバイダ１０１が作成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２が作成したキーファイルＫＦとが格納されている。コンテンツファイルＣＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、コンテンツ鍵データK_cを用いた暗号化されたコンテンツデータＣと、これらについてのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いた署名データとが格納されている。キーファイルＫＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、ライセンス鍵データKD_1～KD_6によって暗号化されたコンテンツ鍵データK_cおよび権利書データ１０６と、これらについてのＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESG,S}$による署名データとが格納されている。なお、図２において、権利書データ１０６は、ライセンス鍵データによって暗号化されていなくてもよい。但し、この場合でも、権利書データ１０６には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いた署名データを付加する。

【００６２】以下、ＥＭＤシステム１００の各構成要素について詳細に説明する。

〔コンテンツプロバイダ１０１〕コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で通信を行う前に、例えば、自らが生成した公開鍵データ$K_{CP,P}$、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでＥＭＤサービスセンタ１０２に登録し、自らの識別子（識別番号）ＣＰ＿ＩＤを得る。また、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESG,P}$と、ルート認証局９２の公開鍵データ$K_{R-CA,P}$とを受ける。

【００６３】コンテンツプロバイダ１０１は、図３（Ａ）に示すコンテンツファイルＣＦと、当該コンテンツファイルＣＦの署名データ$SIG_{6,CP}$と、キーファイルデータベース１１８ｂから読み出した当該コンテンツファイルＣＦに対応する図３（Ｂ）に示すキーファイルＫＦと、当該キーファイルＫＦの署名データ$SIG_{7,CP}$と、記憶部１１９から読み出したコンテンツプロバイダ１０１の公開鍵証明書データ$CER_{CP,P}$と、当該公開鍵証明書データ$CER_{CP,P}$の署名データ$SIG_{1,ESG}$とを格納したセキュアコンテナ１０４を生成する。また、コンテンツプロバイダ１０１は、セキュアコンテナ１０４をオンラインあるいはオフラインで、図１に示すユーザホームネットワーク１０３のネットワーク機器１６$０_1$に供給する。このように、本実施形態では、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書$CER_{CP,P}$をセキュアコンテナ１０４に格納してユーザホームネットワーク１０３に送信するイン・バンド（In-band）方式を採用している。従って、ユーザホームネットワーク１０３は、公開鍵証明書$CER_{CP,P}$を得るための通信をＥＭＤサービスセンタ１０２との間で行う必要がない。なお、本発明では、公開鍵証明書$CER_{CP,P}$をセキュアコンテナ１０４に格納しないで、ユーザホームネットワーク１０３がＥＭＤサービスセンタ１０２から公開鍵証明書$CER_{CP,P}$を得るアウト・オブ・バンド（Out-of-band）方式を採用してもよい。

【００６４】なお、本実施形態では、署名データは、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２および$SAM_1$０５ｉ～１０５ｉの各々において、署名を行なう対象となるデータのハッシュ値をとり、自らの秘密鍵データ$K_{CP,S}$、$K_{ESG,S}$、K_{SAM1}～K_{SAMk}を用いて作成される。ここで、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【００６５】以下、セキュアコンテナ１０４内の各データについて詳細に説明する。

＜署名データ$SIG_{6,CP}$＞署名データ$SIG_{6,CP}$は、セキュアコンテナ１０４の受信先において、コンテンツファイルＣＦの作成者および送信者の正当性を検証するために用いられる。

＜署名データ$SIG_{7,CP}$＞署名データ$SIG_{7,CP}$は、セキュアコンテナ１０４の受信先において、キーファイルＫＦの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ１０４の受信先において、キーファイルＫＦの作成者の正当性の検証は、キーファイルＫＦ内の署名データ$SIG_{1,ESG}$に基づいて行われる。また、署名データ$SIG_{1,ESG}$は、キーファイルＫＦが、ＥＭＤサービスセンタ１０２に登録されているか否かを検証するために用いられる。

【００６６】＜コンテンツファイルＣＦ＞図４は、図３（Ａ）に示すコンテンツファイルＣＦをさらに詳細に説

明するための図である。コンテンツファイルＣＦは、図３（Ａ）および図４に示すように、ヘッダデータと、暗号化部１１４から入力したそれぞれコンテンツ鍵データＫｃで暗号化されたメタデータＭｅｔａ、コンテンツデータＣ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよび電子透かし情報モジュール(Watermark Module)WMとを格納している。なお、図３（Ａ）は、コンテンツデータＣを伸長するＡＶ圧縮伸長用装置として、ＤＳＰ(Digital Signal Processor)を用いた場合のコンテンツファイルＣＦの構成である。当該ＤＳＰでは、セキュアコンテナ１０４内のＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ１０４内のコンテンツデータＣの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ１０１は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。ＡＶ圧縮伸長用装置としてＡ／Ｖ伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルＣＦ内にＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【００６７】ヘッダデータには、図４に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,s}$による署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルＣＦの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関しての情報、およびディレクトリ情報などに関してのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,s}$による署名データが含まれる。

【００６８】メタデータＭｅｔａには、図４に示すように、商品（コンテンツデータＣ）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ１０１による署名データが含まれる。本発明では、図３（Ａ）および図４に示すように、コンテンツファイルＣＦ内にメタデータＭｅｔａを格納して送信する場合を例示するが、メタデータＭｅｔａをコンテンツファイルＣＦ内に格納せずに、コンテンツファイルＣＦを送信する経路とは別の経路でコンテンツプロバイダ１０１からＳＡＭ１０５ｉなどに送信してもよい。

【００６９】コンテンツデータＣは、例えば、コンテンツマスタソースデータベースから読み出したコンテンツデータに対して、ソース電子透かし情報(Source Watermark)Ｗｓ、コピー管理用電子透かし情報(Copy Control Watermark)Ｗｃ、ユーザ電子透かし情報(User Watermark)Ｗｕおよびリンク用電子透かし情報(Link Watermark)ＷＬなどを埋め込んだ後に、例えば、ＡＴＲＡＣ３(Adaptive Transform Acoustic Coding 3)（商標）などの音声圧縮方式で圧縮され、その後、コンテンツ鍵データＫｃを共通鍵として用い、ＤＥＳ(Data Encryption Standard)やＴｒｉｐｌｅ　ＤＥＳなどの共通鍵暗号化方式で暗号化されたデータである。ここで、コンテンツ鍵データＫｃは、例えば、乱数発生器を用いて所定ビット数の乱数を発生して得られる。なお、コンテンツ鍵データＫｃは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データＫｃは、例えば、所定時間毎に更新される。また、複数のコンテンツプロバイダ１０１が存在する場合に、個々のコンテンツプロバイダ１０１によって固有のコンテンツ鍵データＫｃを用いてもよいし、全てのコンテンツプロバイダ１０１に共通のコンテンツ鍵データＫｃを用いてもよい。

【００７０】ソース電子透かし情報Ｗｓは、コンテンツデータの著作権者名、ＩＳＲＣコード、オーサリング目付、オーサリング機器ＩＤ(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Ｗｃは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Ｗｕには、例えば、セキュアコンテナ１０４の配給先および配給先を特定するためのコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよびユーザホームネットワーク１０３のＳＡＭ１０５ｉ～１０５ｎの識別子ＳＡＭ＿ＩＤ１～ＳＡＭ＿ＩＤ$_4$が含まれる。リンク用電子透かし情報(Link Watermark)ＷＬは、例えば、コンテンツデータＣのコンテンツＩＤを含んでいる。リンク用電子透かし情報ＷＬをコンテンツデータＣに埋め込むことで、例えば、テレビジョンやＡＭ／ＦＭラジオなどのアナログ放送でコンテンツデータＣが配信された場合でも、ユーザからの要求に応じて、ＥＭＤサービスセンタ１０２は、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１をユーザに紹介できる。すなち、当該コンテンツデータＣの受信先において、電子透かし情報デコーダを利用したコンテンツデータＣに埋め込まれたリンク用電子透かし情報ＷＬを検出し、当該検出したリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤをＥＭＤサービスセンタ１０２に送信することで、ＥＭＤサービスセンタ１０２は当該ユーザに対して、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などを紹介できる。

【００７１】具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータＣに埋め込まれているリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤや当該コンテンツデータＣを登録しているＥＭＤサービスセンタ１０２の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやＭＤ(Mini Disk)などの光ディスクなどの可搬メディアに搭載されているメディアＳＡＭ

に記録する。そして、当該可搬メディアをネットワークに接続されているＳＡＭを搭載したネットワーク機器をセットする。そして、当該ＳＡＭとＥＭＤサービスセンタ１０２とが相互認証を行った後に、メディアＳＡＭに搭載されている個人情報と、上記記録したコンテンツＩＤなどとをネットワーク機器からＥＭＤサービスセンタ１０２に送信する。その後、ネットワーク機器に、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などの紹介リストなどを、ＥＭＤサービスセンタ１０２から受信する。また、その他に、例えば、ＥＭＤサービスセンタ１０２が、ユーザからコンテンツＩＤなどを受信したときに、当該コンテンツＩＤに対応したコンテンツデータＣを提供しているコンテンツプロバイダ１０１に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ１０１は、当該ユーザが契約者であれば、当該コンテンツデータＣをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【００７２】なお、後述する第２実施形態では、リンク用電子透かし情報ＷＬに基づいて、ＥＭＤサービスセンタ３０２は、ユーザに、当該コンテンツデータＣを扱っているサービスプロバイダ３１０を紹介できる。

【００７３】また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールＷＭとして定義し、ＥＭＤサービスセンタ１０２において電子透かし情報モジュールＷＭを登録して管理する。電子透かし情報モジュールＷＭは、例えば、ユーザホームネットワーク１０３内のネットワーク機器１６０１およびＡＶ機器１６０２～１６０４が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【００７４】Ａ／Ｖ伸長用ソフトウェアＳｏｆｔは、ユーザホームネットワーク１０３のネットワーク機器１６０１およびＡＶ機器１６０２～１６０４において、コンテンツファイルＣＦを伸長する際に用いられるソフトウェアであり、例えば、ＡＴＲＡＣ３方式の伸長用ソフトウェアである。このように、セキュアコンテナ１０４内にＡ／Ｖ伸長用ソフトウェアＳｏｆｔを格納することで、ＳＡＭ１０５１～１０５ｎにおいてセキュアコンテナ１０４内に格納されたＡ／Ｖ伸長用ソフトウェアＳｏｆｔを用いてコンテンツデータＣの伸長を行うことができ、コンテンツデータＣ毎あるいはコンテンツプロバイダ１０１毎にコンテンツデータＣの圧縮および伸長方式

をコンテンツプロバイダ１０１が自由に設定しても、ユーザに多大な負担をかけることはない。

【００７５】また、コンテンツファイルＣＦには、図４に示すように、ファイルリーダと、秘密鍵データ$K_{ED,S}$によるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、ＳＡＭ１０５１～１０５ｎにおいて、異系列の複数のセキュアコンテナ１０４から受信したそれぞれ異なるフォーマットのコンテンツファイルＣＦを格納した複数のセキュアコンテナ１０４を効率的に処理できる。

【００７６】ここで、ファイルリーダは、コンテンツファイルＣＦおよびそれに対応するキーファイルＫＦを読み際に用いられ、これらのファイルの読み込み手順などを示している。但し、本実施形態では、ＥＭＤサービスセンタ１０２からＳＡＭ１０５１～１０５ｎに、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ１０４のコンテンツファイルＣＦは、ファイルリーダを格納していない。

【００７７】本実施形態では、コンテンツデータＣの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータＣを得た信号の標元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータＣがセキュアコンテナ１０４内に格納されている。すなわち、これらの事項をコンテンツプロバイダ１０１が自由に決定できる。

【００７８】＜キーファイルＫＦ＞図５は、図３（Ａ）に示すキーファイルＫＦを詳細に説明するための図である。本実施形態では、例えば、図６に示すように、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に登録用モジュールMod_2が送られて登録処理が行われた後に、例えば６カ月分のキーファイルＫＦがＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に送られ、キーファイルデータベースに格納される。このとき、登録用モジュールMod_2およびキーファイルＫＦの送受信時に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証およびセッション鍵データK_{SES}による暗号化および復号が行われる。キーファイルＫＦは、コンテンツデータＣ修に存在し、後述するように、コンテンツファイルＣＦのヘッダ内のディレクトリ構造データＤＳＤによって、対応するコンテンツファイルＣＦとの間でリンク関係が指定されている。キーファイルＫＦには、図３（Ｂ）および図５に示すように、ヘッダ、コンテンツ鍵データＫｃ、権利書データ（使用許諾条件）１０６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_nおよび署名データ$SIG_{K1,ESC}$が格納されている。ここで、コンテンツプロバイダ１０１の秘密鍵データ$K_{ESC,S}$を用いた

署名データは、図３（Ｂ）に示すようにキーファイルＫＦに格納される全てのデータに対しての署名データ$_{K1,ESG}$にしてもよいし、図５に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データＫｃおよび権利書データ１０６に対しての署名データと、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣに対しての署名データとを別々に設けてもよい。コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$とは、それぞれ対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_6$を用いて暗号化されている。なお、権利書データ１０６は、キーファイルＫＦ内に格納しないでもよい。この場合には、例えば、権利書データ１０６はライセンス鍵データによる暗号化を行わずに、署名データを付加する。

【００７９】ヘッダデータには、図５に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データ$K_{ESG,S}$による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルＫＦに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ１０１の秘密鍵データ$K_{ESG,S}$による署名データが含まれる。なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図７に示すような情報を含めてもよい。また、コンテンツＩＤには、例えば、図８に示す情報が含まれている。コンテンツＩＤは、ＥＭＤサービスセンタ１０２あるいはコンテンツプロバイダ１０１において作成され、ＥＭＤサービスセンタ１０２において作成された場合には図８に示すようにＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESG,S}$による署名データが添付され、コンテンツプロバイダ１０１において作成された場合にはコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$が添付される。コンテンツＩＤは、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の何れで作成してもよい。

【００８０】ディレクトリ構造データは、セキュアコンテナ１０４内におけるコンテンツファイルＣＦ相互間の対応関係と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。例えば、セキュアコンテナ１０４内にコンテンツファイルＣＦ$_1$～ＣＦ$_3$と、それらに対応するキーファイルＫＦ$_1$～ＫＦ$_3$が格納されている場合には、図９に示すように、コンテンツファイルＣＦ$_1$～ＣＦ$_3$相互間のリンクと、コンテンツファイルＣＦ$_1$～ＣＦ$_3$とキーファイルＫＦ$_1$～ＫＦ$_3$との間のリンク関係とがディレクトリ構造データによって確立される。ハイパーリンクデータは、セキュアコンテナ１０４の内外の全てのファイルを対象として、キーファイルＫＦ相互間での階層構造と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。具体的には、図１０に示すように、セキュアコンテナ１０４内にコンテンツファイルＣＦおよびキーファイルＫＦ毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数Ｈ（ｘ）を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【００８１】また、権利書データ１０６は、コンテンツデータＣの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ１０１の運用者が希望する卸売価格やコンテンツデータＣの複製ルールなどが記述されている。具体的には、権利書データ１０６には、図５に示すように、コンテンツＩＤ、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、権利書データ１０６の有効期限、ＥＭＤサービスセンタ１０２の通信アドレス、利用空間調査情報、卸売価格情報ＳＲＰ（Suggested Retailer' Price）、取扱方針、取扱制御情報（Usage Control）、商品デモ（試聴）の取扱制御情報およびそれらについての署名データなどが含まれる。ここで、取扱制御情報は、例えば、再配付（Re-Distribution）、再生課金（PayPer Use）、完全買い切り（Sell Through）、時間制限買い切り（Time Limited Sell Through）、回数制限買い切り（Shell Through Pay Per Play N）、時間課金（Pay Per Time）、ＳＣＭＳ機器への再生課金、ブロック課金（Pay Per Block）などの購入形態のうち許諾された購入形態を示す情報である。

【００８２】なお、後述する第２実施形態のように、サービスプロバイダ３１０を介してユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する場合には、権利書データ１０６には、コンテンツプロバイダ３０１がセキュアコンテナ１０４を提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤが含まれる。

【００８３】また、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$には、図５に示すように、ＳＡＭ１０５$_1$～１０５$_4$内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ（ＵＣＰ）Ｕ１０６のシンタックス（文法）を示すＵＣＰ－Ｌ（Label）、Ｒ（Reader）などのラベルリーダと、ＳＡＭ１０５$_1$～１０５$_4$に内蔵された記憶部１９２（マスクＲＯＭ１１０４、不揮発性メモリ１１０５などのフラッシュＲＯＭ）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。ＳＡＭ１０５$_1$～１０５$_4$のマスクＲＯＭ１１０４およびフラッシュメモリ１１０５では、ロック鍵データに基づいて、記憶データの書き換えおよび消去を許可するか否かをブロック単位で制御する。

【００８４】以下、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を供給する形態について説明する。コンテンツプロバ

イダ１０１は、前述したように、セキュアコンテナ１０４を、オフラインおよび／またはオンラインでユーザホームネットワーク１０３に供給する。コンテンツプロバイダ１０１は、オンラインで、セキュアコンテナ１０４をユーザホームネットワーク１０３のネットワーク機器１６０１に供給する場合には、ネットワーク機器１６０１との間で相互認証を行ってセッション鍵（共通鍵）データK_{SES}を共有し、セキュアコンテナ１０４を当該セッション鍵データK_{SES}を用いて暗号化してEMDサービスセンタ１０２に送信する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。このとき、セキュアコンテナ１０４を送信する通信プロコトルとして、デジタル放送であればMHEG(Multimedia and Hypermedia Information coding Experts Group)プロトコルを用い、インターネットであればXML／SMIL／HTML(Hyper TextMarkup Language)を用い、これらの通信プロトコル内に、セキュアコンテナ１０４を、符号化方式に依存しない形式でトンネリングして埋め込む。従って、通信プロコトルとセキュアコンテナ１０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ１０４のフォーマットを柔軟に設定できる。なお、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。本実施形態では、コンテンツプロバイダ１０１、EMDサービスセンタ１０２およびネットワーク機器１６０１に内蔵された相互間で通信を行うためのモジュールとして、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００８５】また、コンテンツプロバイダ１０１は、オフラインで、セキュアコンテナ１０４をユーザホームネットワーク１０３に供給する場合には、以下に示すようなROM型あるいはRAM型の記録媒体にセキュアコンテナ１０４を記録して、当該記録媒体を所定の流通経路を経てユーザホームネットワーク１０３に供給する。図１１は、本実施形態で用いられるROM型の記録媒体１３０１を説明するための図である。図１１に示すように、ROM型の記録媒体１３０１は、ROM領域１３１、セキュアRAM領域１３２およびメディアＳＡＭ１３３を有する。ROM領域１３１には、図３（Ａ）に示したコンテンツファイルCFが記憶されている。また、セキュアRAM領域１３２は、記憶データに対してのアクセスに所定の許可（認証）が必要な領域であり、図３（Ｂ）、（Ｃ）に示したキーファイルKFおよび公開鍵証明書データCERepと機器の種類に応じて固有の値を持つ記録用鍵データK_{STR}とを引数としてMAC(Message Authentication Code)関数を用いて生成した署名データと、当該キーファイルKFおよび公開鍵証明書データCERepとを記録媒体に固有の値を持つメディア鍵データK_{MED}を用いて暗号化したデータとが記憶される。また、セキュアRAM領域１３２には、例えば、不正行為などで無効となったコンテンツプロバイダ１０１およびＳＡＭ10_{5_1}～10_{5_5}を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。本実施形態で用いられるメディアＳＡＭおよび後述するメディア・ドラブＳＡＭ２６０では、これら相互間で通信を行う際に、自らが持つリボケーションリストと相手方が持つリボケーションリストとの作成時を比較し、自らが持つリボケーションリストの作成時が前の場合には、相手方が持つリボケーションリストによって自らのリボケーションリストを更新する。また、セキュアRAM領域１３２には、後述するようにユーザホームネットワーク１０３のＳＡＭ10_{5_1}～10_{5_4}においてコンテンツデータCoの購入・利用形態が決定されたときに生成される利用制御状態（UCS）データ１６６などが記憶される。これにより、利用制御データ１６６がセキュアRAM領域１３２に記憶されることで、購入・利用形態が決定したROM型の記録媒体130_1となる。メディアＳＡＭ１３３には、例えば、ROM型の記録媒体130_1の識別子であるメディアＩＤと、メディア鍵データK_{MED}とが記憶されている。メディアＳＡＭ１３３は、例えば、相互認証機能を有している。

【００８６】本実施形態で用いるROM型の記録媒体としては、例えば、図１１に示すものの他に、図１２に示すROM型の記録媒体130_2および図１３に示すROM型の記録媒体130_3なども考えられる。図１２に示すROM型の記録媒体130_2は、ROM領域１３１と認証機能を有するメディアＳＡＭ１３３とを有し、図１１に示すROM型の記録媒体130_1のようにセキュアRAM領域１３２を備えていない。ROM型の記録媒体130_2を用いる場合には、ROM領域１３１にコンテンツファイルCFを記録し、メディアＳＡＭ１３３にキーファイルKFを記憶する。また、図１３に示すROM型の記録媒体130_3は、ROM領域１３１およびセキュアRAM領域１３２を有し、図１１に示すROM型の記録媒体130_1のようにメディアＳＡＭ１３３を有していない。ROM型の記録媒体130_3を用いる場合には、ROM領域１３１にコンテンツファイルCFを記録し、セキュアRAM領域１３２にキーファイルKFを記録する。また、ROM型の記録媒体130_3を用いる場合には、ＳＡＭとの間で相互認証は行わない。また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いられる。

【００８７】本実施形態で用いるRAM型の記録媒体としては、例えば図１４に示すように、メディアＳＡＭ１３３、セキュアRAM領域１３２およびセキュアでないRAM領域１３４を有するRAM型の記録媒体130_4がある。RAM型の記録媒体130_4では、メディアＳ

ＡＭ１３３は認証機能を持ち、キーファイルＫＦを記憶する。また、ＲＡＭ領域１３４には、コンテンツファイルＣＦが記録される。また、本実施形態で用いるＲＡＭ型の記録媒体としては、その他に、図１５に示すＲＡＭ型の記録媒体１３５０ｓおよび図１６に示すＲＡＭ型の記録媒体１３０６なども考えられる。図１５に示すＲＡＭ型の記録媒体１３０５は、セキュアでないＲＡＭ領域１３４と認証機能を有するメディアＳＡＭ１３３とを有し、図１４に示すＲＡＭ型の記録媒体１３０４のようにセキュアＲＡＭ領域１３２を備えていない。ＲＡＭ型の記録媒体１３０５を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、メディアＳＡＭ１３３にキーファイルＫＦを記憶する。また、図１６に示すＲＡＭ型の記録媒体１３０６は、セキュアＲＡＭ領域１３２およびセキュアでないＲＡＭ領域１３４を有し、図１４に示すＲＡＭ型の記録媒体１３０４のようにメディアＳＡＭ１３３を有していない。ＲＡＭ型の記録媒体１３０４を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、セキュアＲＡＭ領域１３２にキーファイルＫＦを記録する。また、ＲＡＭ型の記録媒体１３０５を用いる場合には、ＳＡＭとの間で相互認証は行わない。

【００８８】ここで、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配信は、上述したように記録媒体１３０１を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ１０６が格納された共通の形式のセキュアコンテナ１０４を用いる。従って、ユーザホームネットワーク１０３のＳＡＭ１０５１～１０５４では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ１０６に基づいた権利処理を行なうことができる。

【００８９】また、上述したように、本実施形態では、セキュアコンテナ１０４内に、コンテンツ鍵データＫｃ‥で暗号化されたコンテンツデータＣと、当該暗号化を解くためのコンテンツ鍵データＫｃとを同封するイン・バンド(In-Band) 方式を採用している。イン・バンド方式では、ユーザホームネットワーク１０３の機器で、コンテンツデータＣを再生しようとするときに、コンテンツ鍵データＫｃを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データＫｃはライセンス鍵データＫＤ１～ＫＤ６で暗号化されているが、ライセンス鍵データＫＤ１～ＫＤ６は、ＥＭＤサービスセンタ１０２で管理されており、ユーザホームネットワーク１０３のＳＡＭ１０５１～１０５５に事前に（ＳＡＭ１０５１～１０５４がＥＭＤサービスセンタ１０２に初回にアクセスする際に）配信されているので、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２との間をオンラインで接続することなく、オフラインで、コンテンツデータＣの利用が可能になる。なお、本発明は、後述するようにコンテンツデータＣとコンテンツ鍵データＫｃとを別々に、ユーザホームネットワーク１０３に供給するアウト・オブ・バンド(Out-Of-Band) 方式を採用できる柔軟性を有している。

【００９０】以下、コンテンツプロバイダ１０１におけるセキュアコンテナ１０４の作成に係わる処理の流れを説明する。図１７，図１８，図１９は、当該処理の流れを説明するためのフローチャートである。

ステップＳ１７－１：コンテンツプロバイダ１０１の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ１０２に登録処理を行い、グローバルユニークな識別子ＣＰ＿ＩＤを得ている。また、コンテンツプロバイダ１０１は、予め自らの公開鍵証明書データＣＥＲｃｐをＥＭＤサービスセンタ１０２から得ている。

ステップＳ１７－２：コンテンツプロバイダ１０１は、新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツＩＤを割り振り、コンテンツマスタソースデータベースに格納して一元的に管理する。

ステップＳ１７－３：コンテンツプロバイダ１０１は、ステップＳ１７－２において一元的に管理した各々のコンテンツマスタソースにメタデータＭｅｔａを作成し、これをメタデータデータベースに格納して管理する。

【００９１】ステップＳ１７－４：コンテンツプロバイダ１０１は、コンテンツマスタソースデータベースからコンテンツマスタソースであるコンテンツデータを読み出して電子透かし情報を埋め込む。

ステップＳ１７－５：コンテンツプロバイダ１０１は、ステップＳ１７－４で埋め込んだ電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップＳ１７－６：電子透かし情報が埋め込まれたコンテンツデータを圧縮する。

ステップＳ１７－７：コンテンツプロバイダ１０１は、ステップＳ１７－６で圧縮したコンテンツデータを仲長してコンテンツデータを生成する。

ステップＳ１７－８：コンテンツプロバイダ１０１は、伸長したコンテンツデータの聴覚検査を行う。

ステップＳ１７－９：コンテンツプロバイダ１０１は、コンテンツデータに埋め込まれた電子透かし情報を、ステップＳ１７－５でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。そして、コンテンツプロバイダ１０１は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップＳ１７－１０の処理を行い、何れか一方が失敗した場合にはステップＳ１７－４の処理を繰り返す。

【００９２】ステップＳ１７－１０：コンテンツプロバイダ１０１は、乱数を発生してコンテンツ鍵データＫｃ

を生成し、これを保持する。また、コンテンツプロバイダ１０１は、ステップＳ１７－６で圧縮したコンテンツデータを、コンテンツ鍵データＫｃを用いて暗号化する。

【００９３】ステップＳ１７－１１：コンテンツプロバイダ１０１は、図４（Ａ）に示すコンテンツファイルＣＦを作成し、これをコンテンツファイルデータベースに格納する。

【００９４】ステップＳ１７－１２：コンテンツプロバイダ１０１は、コンテンツデータＣについての権利書データ１０６を作成する。

ステップＳ１７－１３：コンテンツプロバイダ１０１は、ＳＲＰを決定する。

ステップＳ１７－１４：コンテンツプロバイダ１０１は、コンテンツＩＤ、コンテンツ鍵データＫｃおよび権利書データ１０６をＥＭＤサービスセンタ１０２に出力する。

ステップＳ１７－１５：コンテンツプロバイダ１０１は、ライセンス鍵データＫＤ$_1$～ＫＤ$_3$で暗号化されたキーファイルＫＦをＥＭＤサービスセンタ１０２から入力する。

ステップＳ１７－１６：コンテンツプロバイダ１０１は、入力したキーファイルＫＦをキーファイルデータベースに格納する。

【００９５】ステップＳ１７－１７：コンテンツプロバイダ１０１は、コンテンツファイルＣＦとキーファイルＫＦとのリンク関係をハイパーリンクで結ぶ。

ステップＳ１７－１８：コンテンツプロバイダ１０１は、コンテンツファイルＣＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{S,CP}$を生成する。また、コンテンツプロバイダ１０１は、キーファイルＫＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{7,CP}$を生成する。

【００９６】ステップＳ１７－１９：コンテンツプロバイダ１０１は、図４に示すように、コンテンツファイルＣＦ、キーファイルＫＦ、公開鍵証明書データＣＥＲ$_{CP}$、署名データ$SIG_{S,CP}$、$SIG_{7,CP}$、$SIG_{1,ESG}$を格納したセキュアコンテナ１０４を作成する。

【００９７】ステップＳ１７－２０：複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップＳ１７－１～Ｂ１９の処理を繰り返して各々のセキュアコンテナ１０４を作成し、コンテンツファイルＣＦとキーファイルＫＦとの間のリンク関係と、コンテンツファイルＣＦ相互間のリンク関係とをハイパーリンクなどを用いて結ぶ。

ステップＳ１７－２１：コンテンツプロバイダ１０１は、作成したセキュアコンテナ１０４をセキュアコンテナデータベースに格納する。

【００９８】［ＥＭＤサービスセンタ１０２］図２０は、ＥＭＤサービスセンタ１０２の主な機能を示す図である。ＥＭＤサービスセンタ１０２は、主に、図２０に示すように、ライセンス鍵データをコンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$に供給する処理と、公開鍵証明書データＣＥＲ$_{CP}$、ＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$の発行処理と、キーファイルＫＦの発行処理、利用履歴データ１０８に基づいた決済処理（利益分配処理）とを行う。

【００９９】＜ライセンス鍵データの供給処理＞先ず、ＥＭＤサービスセンタ１０２からユーザホームネットワーク１０３内のＳＡＭ１０５$_1$～１０５$_4$にライセンス鍵データを送信する際の処理の流れを説明する。ＥＭＤサービスセンタ１０２では、所定期間毎に、例えば、３カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_3$を鍵データベースから読み出して、各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESG,S}$を用いて、それぞれに対応する署名データ$SIG_{KD1,ESG}$～$SIG_{KD3,ESG}$を作成する。そして、ＥＭＤサービスセンタ１０２は、３カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_3$およびそれらの署名データ$SIG_{KD1,ESG}$～$SIG_{KD3,ESG}$を、ＳＡＭ１０５$_1$～１０５$_4$との相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、ＳＡＭ１０５$_1$～１０５$_4$に送信する。また、同様に、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１に、例えば、６カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_6$を送信する。

【０１００】＜公開鍵証明書データの発行処理＞次に、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１から、公開鍵証明書データＣＥＲ$_{CP}$の発行要求を受けた場合の処理を説明する。ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、公開鍵データ$K_{CP,P}$および署名データ$SIG_{S,CP}$をコンテンツプロバイダ１０１から受信すると、これらを、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データ$SIG_{S,CP}$の正当性を検証した後に、識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ１０１がＣＰデータベースに登録されているか否かを確認する。そして、ＥＭＤサービスセンタ１０２は、当該コンテンツプロバイダ１０１のＸ．５０９形式の公開鍵証明書データＣＥＲ$_{CP}$を証明書データベースから読み出し、公開鍵証明書データＣＥＲ$_{CP}$のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESG,S}$を用いて、署名データ$SIG_{1,ESG}$を作成する。そして、ＥＭＤサービスセンタ１０２は、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データ$SIG_{1,ESG}$を、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１０１】なお、ＥＭＤサービスセンタ１０２がＳＡＭ１０５１から、公開鍵証明書データＣＥＲSAM１の発行要求を受けた場合の処理も、ＳＡＭ１０５１との間で処理が行われる点を除いて、公開鍵証明書データＣＥＲRPの発行要求を受けた場合の処理と同じである。公開鍵証明書データＣＥＲRPも、Ｘ．５０９形式で記述されている。なお、本発明では、ＥＭＤサービスセンタ１０２は、例えば、ＳＡＭ１０５１のＩＤ荷時に、ＳＡＭ１０５１　の秘密鍵データKSAM１,Sおよび公開鍵データKSAM１,PをＳＡＭ１０５１の記憶部に記憶する場合には、当該出荷時に、公開鍵データKSAM１,Pの公開鍵証明書データＣＥＲSAM１を作成してもよい。このとき、当該出荷時に、公開鍵証明書データＣＥＲSAM１を、ＳＡＭ１０５１の記憶部に記憶してもよい。

【０１０２】＜キーファイルＫＦの発行処理＞ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１から図６に示す登録用モジュールＭｏｄ２を受信すると、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データKSES0を用いて登録用モジュールＭｏｄ２を復号する。そして、ＥＭＤサービスセンタ１０２は、鍵データベースから読み出した公開鍵データKCP,Pを用いて、署名データＳＩGW１,CPの正当性を検証する。次に、ＥＭＤサービスセンタ１０２は、登録用モジュールＭｏｄ２に格納された権利書データ１０６、コンテンツ鍵データＫｃ、電子透かし情報管理データWMおよびＳＲＰを、権利書データベースに登録する。

【０１０３】次に、ＥＭＤサービスセンタ１０２は、鍵サーバから読み出した対応する期間のライセンス鍵データＫＤ１～ＫＤｅ を用いて、コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ１～ＳＤＣ３とを暗号化する。次に、ＥＭＤサービスセンタ１０２は、ヘッダデータと、コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ１～ＳＤＣ３との全体に対してハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データKESC,Sを用いて署名データＳＩGK１,ESCを作成する。次に、ＥＭＤサービスセンタ１０２は、図４（Ｂ）に示すキーファイルＫＦを作成し、これをＫＦデータベースに格納する。次に、ＥＭＤサービスセンタ１０２は、ＫＦデータベースにアクセスを行って得たキーファイルＫＦを、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データKSES0を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１０４】＜決算処理＞次に、ＥＭＤサービスセンタ１０２において行なう決済処理について説明する。ＥＭＤサービスセンタ１０２は、ユーザホームネットワーク１０３の例えばＳＡＭ１０５１から利用履歴データ１０８およびその署名データＳＩG200,SAM１を入力すると、利用履歴データ１０８および署名データＳＩG200,SAM１を、ＳＡＭ１０５１との間の相互認証によって得られたセッション鍵データKSES0を用いて復号し、ＳＡＭ１０５１の公開鍵データKSAM１による署名データＳＩG200,SAM１の検証を行う。

【０１０５】図２１は、利用履歴データ１０８に記述されるデータを説明するための図である。図２１に示すように、利用履歴データ１０８には、例えば、セキュアコンテナ１０４に格納されたコンテンツデータＣに対してＥＭＤサービスセンタ１０２によってグローバルユニークに付された識別子であるＥＳＣ＿コンテンツＩＤ、当該コンテンツデータＣに対してコンテンツプロバイダ１０１によって付された識別子であるＣＰ＿コンテンツＩＤ、セキュアコンテナ１０４の配給を受けたユーザの識別子であるユーザＩＤ、当該ユーザのユーザ情報、セキュアコンテナ１０４の配給を受けたＳＡＭ１０５１～１０５４の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭが属するホームネットワークグループの識別子であるＨＮＧ＿ＩＤ、ディスカウント情報、トレーシング情報、プライスタグ、当該コンテンツデータを提供したコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、紹介業者（ポータル:Portal）ＩＤ、ハードウェア提供者ＩＤ、セキュアコンテナ１０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ１０４の提供に用いられた例えば圧縮方法などの所定のコンポーネントの識別子であるコンポーネントＩＤ、セキュアコンテナ１０４のライセンス所有者の識別子ＬＨ＿ＩＤ、セキュアコンテナ１０４についての決済処理を行うＥＭＤサービスセンタ１０２の識別子ＥＳＣ＿ＩＤなどが記述されている。なお、後述する第２実施形態では、利用履歴データ３０８には、上述した利用履歴データ１０８に記述されたデータに加えて、当該コンテンツデータＣに対してサービスプロバイダ３１０によって付された識別子であるＳＰ＿コンテンツＩＤと、当該コンテンツデータＣを配給したサービスプロバイダ３１０の識別子ＳＰ＿ＩＤとが記述されている。

【０１０６】ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の所有者以外にも、例えば、圧縮方法や配録媒体などのライセンス所有者に、ユーザホームネットワーク１０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ１０７および決済請求権データ１５２を作成する。当該分配率表は、例えば、セキュアコンテナ１０４に格納されたコンテンツデータ毎に作成される。

【０１０７】次に、ＥＭＤサービスセンタ１０２は、利用履歴データ１０８と、権利書データベースから読み出した権利書データ１０６に含まれる標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を生成する。ここで、決済請求権データ１５２は、当該

データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

【０１０８】次に、ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データＳＩＧ$_{SS}$を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。これにより、決済請求権データ１５２に示される金額の金銭が、コンテンツプロバイダ１０１に支払われる。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０１０９】【ユーザホームネットワーク１０３】ユーザホームネットワーク１０３は、図１に示すように、ネットワーク機器１６０$_1$およびＡ／Ｖ機器１６０$_2$～１６０$_4$を有している。ネットワーク機器１６０$_1$は、ＳＡＭ１０５$_1$を内蔵している。また、ＡＶ機器１６０$_2$～１６０$_4$は、それぞれＳＡＭ１０５$_2$～１０５$_4$を内蔵している。ＳＡＭ１０５$_1$～１０５$_4$の相互間は、例えば、ＩＥＥＥ１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。なお、ＡＶ機器１６０$_2$～１６０$_4$は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器１６０$_1$のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク１０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０１１０】以下、ネットワーク機器１６０$_1$について説明する。図２２は、ネットワーク機器１６０$_1$の構成図である。図２２に示すように、ネットワーク機器１６０$_1$は、ＳＡＭ１０５$_1$、通信モジュール１６２、ＡＶ圧縮・伸長用ＳＡＭ１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。

【０１１１】ＳＡＭ１０５$_1$～１０５$_4$は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ１０２との間で通信を行う。ＳＡＭ１０５$_1$～１０５$_4$は、例えば、ＥＭＤサービスセンタ１０２によって仕様および／またはバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、ＳＡＭ１０５$_1$～１０５$_4$のＩＣ(Integrated Circuit)の内部の仕様を知ることはできず、ＥＭＤサービスセンタ１０２が当該ＩＣのインタフェースなどを統一化し、それに従ってネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$に搭載される。

【０１１２】ＳＡＭ１０５$_1$～１０５$_4$は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Registance)性を持ったハードウェアモジュール（ＩＣモジュールなど）、あるいはＣＰＵにおいてソフトウェア（秘密プログラム）を実行して実現される機能モジュールである。ＳＡＭ１０５$_1$～１０５$_4$の機能をＩＣという形で実現する場合は、ＩＣ内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。ＳＡＭをＩＣという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をＳＡＭとして定義してもよい。

【０１１３】以下、ＳＡＭ１０５$_1$の機能について詳細に説明する。なお、ＳＡＭ１０５$_2$～１０５$_4$は、ＳＡＭ１０５$_1$と基本的に同じ機能を有している。図２３は、ＳＡＭ１０５$_1$の機能の構成図である。なお、図２３には、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する処理に関連するデータの流れが示されている。図２３に示すように、ＳＡＭ１０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、コンテンツプロバイダ管理部１８０、ダウンロードメモリ管理部１８２、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、課金処理部１８７、署名処理部１８９、ＳＡＭ管理部１９０、メディアＳＡＭ管理部１９７、作業用メモリ２００および外部メモリ管理部８１１を有する。ここで、コンテンツプロバイダ管理部１８０およびダウンロードメモリ管理部１８２がＡ項発明の入力処理手段に対応し、課金処理部１８７がＡ項発明の決定手段、最履データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部１７２がＡ項発明の復号手段に対応し、利用監視部１８６がＡ項発明の利用制御手段に対応している。また、暗号化・復号部１７３が請求項３等の暗号化手段に対応している。また、後述する例えば図３８に示すメディア・ドライブＳＡＭ管理部８５５がＡ項発明の請求項５等の記録制御手段に対応している。また、署名処理部１８９が請求項９等の署名処理手段に対応している。

【０１１４】なお、図２３に示すＳＡＭ１０５$_1$の各機能は、前述したように、ＣＰＵにおいて秘密プログラムを実行して実現されるか、あるいは所定のハードウェアによって実現される。また、外部メモリ２０１には、以下に示す処理を経て、図２４に示すように、利用履歴データ１０８およびＳＡＭ登録リストが記憶される。ここで、外部メモリ２０１のメモリ空間は、ＳＡＭ１０５$_1$の外部（例えば、図示しないホストＣＰＵ）からは見ることはできず、ＳＡＭ１０５$_1$のみが外部メモリ２０１の記憶領域に対してのアクセスを管理できる。外部メモリ２０１としては、例えば、フラッシュメモリあるいは

強誘電体メモリ（ＦｅＲＡＭ）などが用いられる。また、作業用メモリ２００としては、例えばＳＲＡＭが用いられ、図２５に示すように、セキュアコンテナ１０４、コンテンツ鍵データK_C、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{Loc}、コンテンツプロバイダ１０１の公開鍵証明書CER_{CP}、利用制御データ（ＵＣＳ）１６６、およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3などが記憶される。

【０１１５】以下、$SAM105_1$の機能のうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力したときの各機能ブロックの処理内容を図２３を参照しながら説明する。

【０１１６】相互認証部１７０は、$SAM105_1$がコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間でオンラインでデータを送受信する際に、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成し、これを暗号化・復号部１７１に出力する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【０１１７】暗号化・復号部１７１は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で送受信するデータを、相互認証部１７０が生成したセッション鍵データK_{SES}を用いて暗号化・復号する。

【０１１８】ダウンロードメモリ管理部１８２は、図２２に示すようにダウンロードメモリ１６７が相互認証機能を持つメディアＳＡＭ１６７ａを有している場合には、相互認証部１７０とメディアＳＡＭ１６７ａとの間で相互認証を行った後に、相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化して図２２に示すダウンロードメモリ１６７に書き込む。ダウンロードメモリ１６７としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図２６に示すように、ＨＤＤ(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ２１１として用いる場合には、ダウンロードメモリ２１１内はセキュアではないので、コンテンツファイルＣＦをダウンロードメモリ２１１にダウンロードし、機密性の高いキーファイルＫＦを例えば、図２３に示す作業用メモリ２００あるいは図２２に示す外部メモリ２０１にダウンロードする。キーファイルＫＦを外部メモリ２０１に記憶する場合には、例えば、$SAM105_1$において、キーファイルＫＦをＣＢＣモードでMAC_{KMAC}鍵データK_{MAC}を用いて暗号化して外部メモリ２０１に記憶し、最後の暗号文ブロックの一部をＭＡＣ(Message Authentication Code)値として$SAM105_1$内に記憶する。そして、外部メモリ２０１から$SAM105_1$にキーファイルＫＦを読み出す場合には、$SAM105_1$内で当該読み出したキーファイルＫＦをMAC_{KMAC}鍵データK_{MAC}を用いて復号し、それによって得たＭＡＣ値と、既に記憶しているＭＡＣ値とを比較することで、キーファイルＫＦが改竄されているか否かを検証する。この場合に、ＭＡＣ値ではなく、ハッシュ値を用いてもよい。

【０１１９】暗号化・復号部１７２は、ダウンロードメモリ管理部１８２から入力したセキュアコンテナ１０４に格納されたキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびSAM_{CP}プログラム・ダウンロード・コンテナSDC_1～SDC_3を、記憶部１９２から読み出した対応する期間のライセンス鍵データKD_1～KD_3を用いて復号する。当該復号されたコンテンツ鍵データＫｃ、権利書データ１０６およびSAM_{CP}プログラム・ダウンロード・コンテナSDC_1～SDC_3は、作業用メモリ２００に書き込まれる。

【０１２０】ＥＭＤサービスセンタ管理部１８５は、図１に示すＥＭＤサービスセンタ１０２との間の通信を管理する。

【０１２１】署名処理部１８９は、記憶部１９２から読み出したＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$およびコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４内の署名データの検証を行なう。

【０１２２】記憶部１９２は、$SAM105_1$の外部から読み出しおよび書き換えできない秘密データとして、図２７に示すように、有効期限付きの複数のライセンス鍵データKD_1～KD_3、ＳＡＭ＿ＩＤ、ユーザＩＤ、パスワード、当該ＳＡＭが属するホームネットワークグループの識別子ＨＮＧ＿ＩＤ、情報参照用ＩＤ、ＳＡＭ登録リスト、機器および記憶媒体のリボケーションリスト、記録用鍵データK_{STR}、ルートＣＡの公開鍵データ$K_{R-CA,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ドライブ用ＳＡＭの認証用元鍵（共通鍵暗号化方式を採用した場合）、ドライブ用ＳＡの公開鍵証明書（秘密鍵暗号化方式を採用した場合）、$SAM105_1$の秘密鍵データ$K_{SAM1,S}$（共通鍵暗号化方式を採用した場合）、$SAM105_1$の公開鍵データ$K_{SAM1,P}$を格納した公開鍵証明書CER_{SAM1}（秘密鍵暗号化方式を採用した場合）、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いた公開鍵証明書CER_{ESC}の署名データSIG_{22}、ＡＶ圧縮・伸長用SAM_{163}との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアＳＡＭとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAM_{MEDSAM}（公開鍵暗号化方式を採用した場合）、扱える信号の諸元、圧縮方式、接続するモニタ表示能力、フォーマット変換機能、ビットストリームレコーダが有無、権利処理（利益分配）用データ、利益分配する関連エンティティのＩＤなどを記憶している。なお、図２７において、左側に「＊」を付し

たデータは、ＳＡＭ１０５ｉの出荷時に記憶部１９２に記憶されており、それ以外のデータは出荷後に行われるユーザ登録時に記憶部１９２に記憶される。

【０１２３】また、記憶部１９２には、図２３に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。記憶部１９２としては、例えば、フラッシュＥＥＰＲＯＭ(Electrically Erasable Programmable RAM)が用いられる。

【０１２４】＜ライセンス鍵データの受信時の処理＞以下、ＥＭＤサービスセンタ１０２から受信したライセンス鍵データＫＤｉ～ＫＤ３を記憶部１９２に格納する際のＳＡＭ１０５ｉ内での処理の流れを図２６および図２８を参照しながら説明する。図２８は、ＥＭＤサービスセンタ１０２から受信したライセンス鍵データＫＤｉ～ＫＤ３を記憶部１９２に格納する際のＳＡＭ１０５ｉ内での処理の流れを示すフローチャートである。

ステップＳ２８－１：ＳＡＭ１０５ｉの相互認証部１７０と、ＥＭＤサービスセンタ１０２との間で相互認証を行なう。

ステップＳ２８－２：ステップＳ２８－１の相互認証によって得られたセッション鍵データK_{SES}で暗号化した3カ月分のライセンス鍵データＫＤｉ～ＫＤ３およびその署名データ$SIG_{KDi,ESC}$～$SIG_{KD3,ESC}$を、ＥＭＤサービスセンタ１０２からＥＭＤサービスセンタ管理部１８５を介して作業用メモリ２００に書き込む。

【０１２５】ステップＳ２８－３：暗号化・復号部１７１は、セッション鍵データK_{SES}を用いて、ライセンス鍵データＫＤｉ～ＫＤ３およびその署名データ$SIG_{KDi,ESC}$～$SIG_{KD3,ESC}$を復号する。

ステップＳ２８－４：署名処理部１８９は、作業用メモリ２００に記憶された署名データ$SIG_{KDi,ESC}$～$SIG_{KD3,ESC}$の正当性を確認した後に、ライセンス鍵データＫＤｉ～ＫＤ３を記憶部１９２に書き込む。

【０１２６】＜セキュアコンテナ１０４をコンテンツプロバイダ１０１から入力した時の処理＞以下、コンテンツプロバイダ１０１が提供したセキュアコンテナ１０４を入力する際のＳＡＭ１０５ｉ内での処理の流れを図２３および図２９を参照しながら説明する。なお、以下に示す例では、ＳＡＭ１０５ｉにおいて、セキュアコンテナ１０４を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ１０４の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップＳ２９－１：図２３に示すＳＡＭ１０５ｉの相互認証部１７０とコンテンツプロバイダ１０１との間で相互認証を行なう。

ステップＳ２９－２：ＳＡＭ１０５ｉの相互認証部１７０とダウンロードメモリ１６７のメディアＳＡＭ１６７ａとの間で相互認証を行なう。

【０１２７】ステップＳ２９－３：コンテンツプロバイダ１０１から受信したセキュアコンテナ１０４を、ダウンロードメモリ１６７に書き込む。このとき、ステップＳ２９－２で得られたセッション鍵データを用いて、相互認証部１７０におけるセキュアコンテナ１０４の暗号化と、メディアＳＡＭ１６７ａにおけるセキュアコンテナ１０４の復号とを行なう。

ステップＳ２９－４：ＳＡＭ１０５ｉは、ステップＳ２９－１で得られたセッション鍵データを用いて、セキュアコンテナ１０４の復号を行なう。

【０１２８】ステップＳ２９－５：署名処理部１８９は、図３（Ｃ）に示す署名データ$SIG_{T1,ESC}$の検証を行なった後に、図３（Ｃ）に示す公開鍵証明書データCER_{KCP}内に格納されたコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{S6,CP}$、$SIG_{T7,CP}$の正当性を検証する。このとき、署名データ$SIG_{S6,CP}$が正当であると検証されたときに、コンテンツファイルＣＦの作成者および送信者の正当性が確認される。また、署名データ$SIG_{T7,CP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０１２９】ステップＳ２９－６：署名処理部１８９は、記憶部１９２から読み出した公開鍵データ$K_{ESS,P}$を用いて、図３（Ｂ）に示すキーファイルＫＦ内の署名データ$SIG_{KT1,ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２に業務されているか否かの検証を行う。

【０１３０】ステップＳ２９－７：暗号化・復号部１７２は、記憶部１９２から読み出した対応する期間のライセンス鍵データＫＤｉ～ＫＤ３を用いて、図３（Ｂ）に示すキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣｉ～ＳＤＣ３を復号し、これらを作業用メモリ２００に書き込む。

【０１３１】以下、ダウンロードメモリ１６７にダウンロードされたコンテンツデータＣを利用・購入する処理に関連する各機能ブロックの処理内容を図３０を参照しながら説明する。

【０１３２】利用監視部１８６は、作業用メモリ２００から権利書データ１０６および利用制御データ１６６を読み出し、当該読み出した権利書データ１０６および利用制御データ１６６によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ１０６は、図２９を用いて説明したように、後号後に作業用メモリ２００に記憶されたキーファイルＫＦ内に格納されている。また、利用制御データ１６６は、後述するように、ユーザによって購入形態が決定されたときに、作業用メモリ２００に記憶される。なお、利用制御データ１６６には、当該コンテンツデータ

Ｃを購入したユーザのユーザＩＤおよびトレーシング（Tracing）情報が記述され、取扱制御情報として購入形態決定処理で決定された購入形態が記述されている点を除いて、図３に示す権利書データ１０６と同じデータが記述されている。

【０１３３】課金処理部１８７は、図２３に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５に応じた利用履歴データ１０８を作成する。ここで、利用履歴データ１０８は、前述したように、ユーザによるセキュアコンテナ１０４の購入および利用の形態の履歴を記述しており、ＥＭＤサービスセンタ１０２において、セキュアコンテナ１０４の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【０１３４】また、課金処理部１８７は、必要に応じて、作業用メモリ２００から読み出した販売価格あるいは標準小売価格データＳＲＰをユーザに通知する。ここで、販売価格および標準小売価格データＳＲＰは、復号後に作業用メモリ２００に記憶された図３（Ｂ）に示すキーファイルＫＦの権利書データ１０６内に格納されている。課金処理部１８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【０１３５】また、課金処理部１８７は、操作信号Ｓ１６５に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御（UCS: Usage Control Status）データ１６６を生成し、これを作業用メモリ２００に書き込む。本実施形態では、購入形態を決定した後に、利用制御データ１６６を作業用メモリ２００に記憶する場合を例示したが、利用制御データ１６６およびコンテンツ鍵データＫｃを外付けメモリである外部メモリ２０１に格納するようにしてもよい。外部メモリ２０１としは、前述したように、例えばＮＶＲＡＭであるフラッシュメモリが用いられる。外部メモリ２０１に書き込みを行う場合には外部メモリ２０１の正当性の検証であるインテグリティチェック（Integrity Check）を行うが、この際に外部メモリ２０１の記憶領域を複数のブロックに分け、ブロック毎にＳＨＡ－１あるいはＭＡＣなどでハッシュ値を求め、当該ハッシュ値をＳＡＭ１０５１内で管理する。なお、ＳＡＭ１０５１において、購入形態を決定せずに、セキュアコンテナ１０４を他のＳＡＭ１０５２～１０５４に転送してもよい。この場合には、利用制御データ１６６は作成されない。

【０１３６】コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切り（Sell Through）、利用期間に制限を持たせるタイムリミテッド（Time Limited）、再生する度に課金を行なう再生課金（Pay Per Play）、ＳＣＭＳ機器を用いた複製において再生する度に課金を行なう再生課金（Pay Per SCMS）、ＳＣＭＳ機器において複製を認める（Sell Through SCMSCopy）、および複製のガードを行わずに再生する度に課金を行う再生課金（Pay Per Copy N without copy guard）などがある。ここで、利用制御データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ１６６には、コンテンツのＩＤ、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ、購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０１３７】なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ１０５１からコンテンツプロバイダ１０１に利用制御データ１６６をコンテンツデータＣの購入と同時にリアルタイムに送信し、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２に、利用履歴データ１０８を所定の期間内にＳＡＭ１０５１に取りにいくことを格納する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ１６６が、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御データ１６６をコンテンツプロバイダ１０１にリアルタイムに送信する。

【０１３８】ＥＭＤサービスセンタ管理部１８５は、所定の期間毎に、外部メモリ管理部８１１を介して外部メモリ２０１から読み出した利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信する。このとき、ＥＭＤサービスセンタ管理部１８５は、署名処理部１８９において、秘密鍵データ$K_{SAM1,a}$を用いて利用履歴データ１０８の署名データ$SIG_{00,SAM1}$を作成し、署名データ$SIG_{00,SAM1}$を利用履歴データ１０８と共にＥＭＤサービスセンタ１０２に送信する。ＥＭＤサービスセンタ１０２への利用履歴データ１０８の送信は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ１０８に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ２０１の記憶容量に応じて決定される。

【０１３９】ダウンロードメモリ管理部１８２は、例えば、図２２に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツデータＣ、作業用メモリ２００から読み出したコンテンツ鍵データＫｃおよび課金処理部１８７から入力したユーザ電子透かし情報用データ１９６をＡＶ圧縮・伸長用ＳＡＭ管理部１８４に出力する。また、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４は、図２２に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコン

テンツの試聴動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツファイルＣＦ、並びに作業用メモリ２００から読み出したコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９をＡＶ圧縮・伸長用ＳＡＭ管理部１８４に出力する。

【０１４０】ここで、半開示パラメータデータ１９９は、権利書データ１０６内に記述されており、試聴モード時のコンテンツの取り扱いを示している。ＡＶ圧縮・伸長用ＳＡＭ１６３では、半開示パラメータデータ１９９に基づいて、暗号化されたコンテンツデータＣを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、ＡＶ圧縮・伸長用ＳＡＭ１６３がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ１９９によって、コンテンツ鍵データＫｃを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【０１４１】＜ダウンロードしたセキュアコンテナの購入形態決定処理＞以下、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを図３０および図３１を参照しながら説明する。なお、以下に示す処理では、セキュアコンテナ１０４の購入形態を決定する際に、セキュアコンテナ１０４内の各データの署名データの検証を行わない（前述したようにセキュアコンテナ１０４の受信時に署名データの検証を行う）場合を例示するが、当該購入形態を決定する際にこれらの署名データの検証を行ってもよい。図３１は、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを示すフローチャートである。

ステップＳ３１－１：ユーザによる図２２に示す購入・利用形態決定操作部１６５の操作に応じた試聴モードを示す操作信号Ｓ１６５が課金処理部１８７に出力されたか否かを判断し、出力されたと判断した場合にはステップＳ３１－２の処理を実行し、出力されていないと判断した場合にはステップＳ３１－５の処理を実行する。

【０１４２】ステップＳ３１－２：作業用メモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データＫｓｅｓ による暗号化および復号が行なわれる。

【０１４３】ステップＳ３１－３：ユーザによる図２２に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が課金処理部１８７に出力されると、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４を介して、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７との間の相互認証およびセッション鍵データＫｓｅｓ による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データＫｓｅｓ による暗号化・復号とが行なわれる。コンテンツファイルＣＦは、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データＫｓｅｓ を用いて復号された後に、復号部２２２に出力される。

【０１４４】ステップＳ３１－４：復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。次に、電子透かし情報処理部２２４においてコンテンツデータＣにユーザ電子透かし情報用データ１９６が埋め込まれ、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。また、電子透かし情報処理部２２４では、コンテンツデータＣに埋め込まれている電子透かし情報が検出され、当該検出の結果に基づいて、処理の停止の有無を決定する。

【０１４５】ステップＳ３１－５：ユーザが購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。

ステップＳ３１－６：課金処理部１８７において、決定された購入形態に応じた利用履歴データ１０８および利用制御データ１６６が生成され、利用履歴データ１０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に、利用制御データ１６６が作業用メモリ２００に書き込まれる。以後は、利用監視部１８６において、利用制御データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【０１４６】ステップＳ３１－７：後述する図３２（Ｃ）に示す新たなキーファイルＫＦｉが作成され、当該作成されたキーファイルＫＦｉ がダウンロードメモリ管理部１８２を介してダウンロードメモリ１６７あるいはその他のメモリに記憶される。図３２（Ｃ）に示すように、キーファイルＫＦｉ に格納された利用制御データ１６６はストレージ鍵データＫｓｔｒ およびメディア鍵データＫｍｅｄ を用いてＤＥＳのＣＢＣモードを利用して順に暗号化されている。ここで、記録用鍵データＫ

STR は、例えばＳＡＣＤ(Super Audio Compact Disc)、ＤＶＤ(Digital Versatile Disc)機器、ＣＤ－Ｒ機器およびMD (Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。また、メディア鍵データ K_{MED} は、記録媒体にユニークなデータである。

【０１４７】ステップＳ３１－８：署名処理部１８９において、ＳＡＭ１０５１の秘密鍵データ $K_{SAM1,S}$ を用いて、キーファイルＫＦ１のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイルＫＦ１と対応付けられて作業用メモリ２００に書き込まれる。ハッシュ値 H_{K1} は、キーファイルＫＦ１の作成者の正当性およびキーファイルＫＦ１が改竄されたか否かを検証するために用いられる。なお、購入形態が決定されたコンテンツデータＣを、例えば、記録媒体に記録したり、オンラインを介して送信する場合には、図３２に示すように、キーファイルＫＦ１およびハッシュ値 H_{K1}、コンテンツファイルＣＦおよびその署名データ $SIG_{6.CF}$、キーファイルＫＦおよびその署名データ $SIG_{7.CF}$、公開鍵証明書データ CER_{MP} およびその署名データ $SIG_{1.ESC}$、公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{22.ESC}$ を格納したセキュアコンテナ１０４ｐが作成される。上述したようにセキュアコンテナ１０４の購入形態を決定すると、利用制御データ１６６が生成されて作業用メモリ２００に記憶されるが、ＳＡＭ１０５１に対しては再び同じセキュアコンテナ１０４について購入形態を再決定する場合には、操作信号Ｓ１６５に応じて作業用メモリ２００に記憶されている利用制御データ１６６が更新される。

【０１４８】＜コンテンツデータの再生処理＞次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図３３を参照しながら説明する。図３３は、当該処理を示すフローチャートである。当該処理を行う前提として、前述した購入形態の決定処理によって作業用メモリ２００に、利用制御データ１６６が格納されている。

ステップＳ３３－１：作業用メモリ２００から利用監視部１８６に、利用制御データ１６６が読み出され、利用制御データ１６６が示す再生条件が解釈・検証され、その結果に基づいて以後の再生処理が行われるように監視される。

ステップＳ３３－２：図３０に示す相互認証部１７０と、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の相互認証部２２０との間で相互に認証が行われ、セッション鍵データ K_{SES} が共有される。

【０１４９】ステップＳ３３－３：ステップＳ３３－１で解釈・検証された再生条件と、作業用メモリ２００から読み出されたコンテンツ鍵データＫｃとが、ステップＳ３３－２で得られたセッション鍵データ K_{SES} を用いて暗号化された後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。これによって、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データ K_{SES} を用いて再生条件およびコンテンツ鍵データＫｃが復号される。

【０１５０】ステップＳ３３－４：ダウンロードメモリ１６７から読み出されたコンテンツファイルＣＦが、ステップＳ３３－２で得られたセッション鍵データ K_{SES} を用いて暗号化された後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。これによって、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データ K_{SES} を用いてコンテンツファイルＣＦが復号される。続いて、ＡＶ圧縮・伸長用ＳＡＭ１６３の伸長部２２３において、コンテンツファイルＣＦ内のコンテンツデータＣが伸長され、電子透かし情報処理部２２４においてユーザ電子透かし情報を埋め込んだ後に再生モジュール１６９において再生される。

【０１５１】ステップＳ３３－５：必要に応じて、ステップＳ３３－１で読み出された利用制御データ１６６が更新され、再び作業用メモリ２００に書き込まれる。また、外部メモリ２０１に記憶されている利用履歴データ１０８も更新される。

【０１５２】＜一の機器の利用制御　態データ（ＵＳＣ）１６６を使用して他の機器で再購入を行う場合の処理＞先ず、図３４に示すように、例えば、ネットワーク機器１６０１のダウンロードメモリ１６７にダウンロードされたコンテンツファイルＣＦの購入形態を前述したように決定した後に、当該コンテンツファイルＣＦを格納した新たなセキュアコンテナ１０４ｘを生成し、バス１９１を介して、ＡＶ機器１６０２のＳＡＭ１０５２にセキュアコンテナ１０４ｘを転送するまでのＳＡＭ１０５１内での処理の流れを図３５および図３６を参照しながら説明する。

【０１５３】図３６は、当該処理のフローチャートである。図３６に示す処理を行う前提として、前述した購入処理によって、ＳＡＭ１０５１の作業用メモリ２００には図３２（Ｃ）に示すキーファイルＫＦ１およびハッシュ値 H_{K1} が記憶されている。

ステップＳ３６－１：ユーザは、購入・利用形態決定操作部１６５を操作して、購入形態を既に決定したセキュアコンテナをＳＡＭ１０５２に転送することを指示する。課金処理部１８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。

【０１５４】ステップＳ３６－２：ＳＡＭ１０５１は、後述するＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ１０５２が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ３６－３以降の処理を行う。また、ＳＡＭ１０５１は、ＳＡＭ１０５２がホームネット

ワーク内のＳＡＭであるか否かの検証も行う。

【０１５５】ステップＳ３６－３：相互認証部１７０は、ＳＡＭ１０５$_2$との間で相互認証を行って得たセッション鍵データK_{SES}を共用する。

【０１５６】ステップＳ３６－４：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図３２（Ａ）に示すコンテンツファイルＣＦおよび署名データ$SIG_{6.CP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データK_{SAM1}を用いた署名データ$SIG_{41.SAM1}$を署名処理部１８９に作成させる。

【０１５７】ステップＳ３６－５：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図３２（Ｂ）に示すキーファイルＫＦおよび署名データ$SIG_{7.CP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データK_{SAM1}を用いた署名データ$SIG_{42.SAM1}$を署名処理部１８９に作成させる。

【０１５８】ステップＳ３６－６：ＳＡＭ管理部１９０は、図３７に示すセキュアコンテナ１０４ｘを作成する。

ステップＳ３６－７：暗号化・復号部１７１において、ステップＳ３６－３で得たセッション鍵データK_{SES}を用いて、図３７に示すセキュアコンテナ１０４ｘが暗号化される。

【０１５９】ステップＳ３６－８：ＳＡＭ管理部１９０は、セキュアコンテナ１０４ｘを図３４に示すＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力する。これとき、ＳＡＭ１０５$_1$とＳＡＭ１０５$_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０１６０】以下、図３４に示すように、ＳＡＭ１０５$_1$から入力した図３７に示すセキュアコンテナ１０４ｘを、ＲＡＭ型などの記録媒体（メディア）１３０４に蓄き込む際のＳＡＭ１０５$_2$内での処理の流れを図３８、図３９および図４０を参照して説明する。図３９および図４０は、当該処理を示すフローチャートである。ここで、ＲＡＭ型の記録媒体１３０４は、例えば、セキュアでないＲＡＭ領域１３４、メディアＳＡＭ１３３およびセキュアＲＡＭ領域１３２を有している。

【０１６１】ステップＳ３９－１：ＳＡＭ１０５$_2$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送元のＳＡＭ１０５$_1$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ３９－２以降の処理を行う。また、ＳＡＭ１０５$_2$は、ＳＡＭ１０５$_1$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０１６２】ステップＳ３９－２：前述したステップＳ３６－２に対応する処理として、ＳＡＭ１０５$_2$は、ＳＡＭ１０５$_1$との間で相互認証を行って得たセッション鍵データK_{SES}を共用する。

ステップＳ３９－３：ＳＡＭ１０５$_2$のＳＡＭ管理部１９０は、図３４および図３８に示すように、ネットワーク機器１６０$_1$のＳＡＭ１０５$_1$からセキュアコンテナ１０４ｘを入力する。

ステップＳ３９－４：暗号化・復号部１７１は、ステップＳ３９－２で共用したセッション鍵データK_{SES}を用いて、ＳＡＭ管理部１９０を介して入力したセキュアコンテナ１０４ｘを復号する。

【０１６３】ステップＳ３９－５：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ１０４ｘ内のコンテンツファイルＣＦが、図３２に示すメディア・ドラブＳＡＭ２６０におけるセクタライズ（Sectorize）、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体１３０４のＲＡＭ領域１３４に記録される。

【０１６４】ステップＳ３９－６：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ１０４ｘ内の署名データ$SIG_{6.CP}$、$SIG_{41.SAM1}$と、キーファイルＫＦおよびその署名データ$SIG_{7.CP}$、$SIG_{42.SAM1}$と、キーファイルＫＦ$_1$およびそのハッシュ値H_{K1}と、公開鍵署名データCER_{ICP}およびその署名データ$SIG_{1.ESC}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22.ESC}$とが、作業用メモリ２００に書き込まれる。

【０１６５】ステップＳ３９－７：署名処理部１８９において、記憶部１９２から読み出した公開鍵データK_{CP},$_P$を用いて、公開鍵証明書データCER_{ICP}，CER_{SAM1}の正当性が確認される。そして、署名処理部１８９において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{CP},$_P$を用いて、署名データ$SIG_{6.CP}$の正当性が検証され、コンテンツファイルＣＦの作成者の正当性が確認される。また、署名処理部１８９において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1},$_P$を用いて、署名データ$SIG_{41.SAM1}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。

【０１６６】ステップＳ３９－８：署名処理部１８９は、公開鍵データK_{CP}，K_{SAM1},$_P$を用いて、作業用メモリ２００に記憶されている署名データ$SIG_{7.CP}$，$SIG_{42.SAM1}$の正当性を検証する。そして、署名データ$SIG_{7.CP}$，$SIG_{42.SAM1}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０１６７】ステップＳ３９－９：署名処理部１８９は、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、図３７（Ｂ）に示すキーファイルＫＦに格納された署名データ$SIG_{K1.ESC}$の正当性を確認する。そして、署名データ$SIG_{K1.ESC}$が正当であると検証されたときに、キーファイルＫＦの作成者の正当性が確認される。

【０１６８】ステップＳ３９－１０：署名処理部１８９は、ハッシュ値H_{K1}の正当性を検証し、キーファイルK_{F1}の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルK_{F1}の作成者と送信元とが同じ場合を述べたが、キーファイルK_{F1}の作成者と送信元とが異なる場合には、キーファイルK_{F1}に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０１６９】ステップＳ３９－１１：利用監視部１８６は、ステップＳ３９－１０で復号されたキーファイルK_{F1}に格納された利用制御データ１６６を用いて、以後のコンテンツデータＣの購入・利用形態を制御する。

【０１７０】ステップＳ３９－１２：ユーザは、購入・利用形態決定操作部１６５を操作して購入形態を決定し、当該操作に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。

ステップＳ３９－１３：課金処理部１８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。また、課金処理部１８７は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ１６６を更新する。

【０１７１】ステップＳ３９－１４：暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を順に用いて、ステップＳ３９－１２で生成された利用制御データ１６６を暗号化してメディア・ドライブＳＡＭ管理部８５５に出力する。

ステップＳ３９－１５：メディア・ドライブＳＡＭ管理部８５５は、新たな利用制御データ１６６を格納したキーファイルK_{F1}を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体１３０４のセキュアＲＡＭ領域１３２に記録する。なお、メディア鍵データK_{MED}は、図３８に示す相互認証部１７０と図３４に示すＲＡＭ型の記録媒体１３０４のメディアＳＡＭ１３３との間の相互認証によって記憶部１９２に事前に記憶されている。

【０１７２】ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ（Super Audio Compact Disc）、ＤＶＤ（Digital Versatile Disc）機器、ＣＤ－Ｒ機器およびＭＤ（Mini Disc）機器などの種類（当該例では、ＡＶ機器１６０$_2$）に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。なお、ＳＡＣＤとＤＶＤとでは、ディスク媒体の物理的な構造が同じであるため、ＤＶＤ機器を用いてＳＡＣＤの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。なお、本実施形態では、記録用鍵データK_{STR}を用いた暗号化を行わないようにしてもよい。

【０１７３】また、メディア鍵データK_{MED}は、記録媒体（当該例では、ＲＡＭ型の記録媒体１３０４）にユニークなデータである。メディア鍵データK_{MED}は、記録媒体（当該例では、図３４に示すＲＡＭ型の記録媒体１３０４）側に格納されており、記録機器のメディアＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアＳＡＭが搭載されている場合には、当該メディアＳＡＭ内に記憶されており、記録媒体にメディアＳＡＭが搭載されていない場合には、例えば、ＲＡＭ領域内の図示しないホストＣＰＵの管理外の領域に記憶されている。なお、本実施形態のように、機器側のＳＡＭ（当該例では、ＳＡＭ１０５$_2$）とメディアＳＡＭ（当該例では、メディアＳＡＭ１３３）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のＳＡＭに転送し、機器側のＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【０１７４】また、購入者鍵データK_{PIN}は、コンテンツファイルＣＦの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してＥＭＤサービスセンタ１０２によって割り当てられる。購入者鍵データK_{PIN}は、ＥＭＤサービスセンタ１０２において管理される。

【０１７５】ステップＳ３９－１６：キーファイルＫＦが作業用メモリ２００から読み出され、メディア・ドライブＳＡＭ管理部８５５を介して、図３４に示すメディア・ドラブＳＡＭ２６０によってＲＡＭ型の記録媒体１３０４のセキュアＲＡＭ領域１３２に書き込まれる。

【０１７６】また、上述した実施形態では、メディア・ドラブＳＡＭ２６０による処理を経て、キーファイルＫＦ，K_{F1}をＲＡＭ型の記録媒体１３０４のセキュアＲＡＭ領域１３２に記録する場合を例示したが、図３４において点線で示すように、ＳＡＭ１０５$_2$からメディアＳＡＭ１３３にキーファイルＫＦ，K_{F1}を記録するようにしてもよい。

【０１７７】また、上述した実施形態では、ＳＡＭ１０５$_1$からＳＡＭ１０５$_2$にセキュアコンテナ１０４$_x$を送信する場合を例示したが、ネットワーク機器１６０$_1$のホストＣＰＵおよびＡＶ機器１６０$_2$のホストＣＰＵによって、コンテンツファイルＣＦおよび権利書データ１０６をネットワーク機器１６０$_1$からＡＶ機器１６０$_2$に送信してもよい。この場合には、ＳＡＭ１０５$_1$からＳＡＭ１０５$_2$に、利用制御データ１６６およびコンテンツ鍵データK_cが送信される。

63

【０１７８】また、その他の実施形態として、例えば、ＳＡＭ１０５１において購入形態を決定し、ＳＡＭ１０５２では購入形態を決定せずに、ＳＡＭ１０５１において生成した利用制御データ１６６をＳＡＭ１０５２でそのまま用いてもよい。この場合には、利用履歴データ１０８は、ＳＡＭ１０５１において生成され、ＳＡＭ１０５２では生成されない。また、コンテンツデータＣの購入は、例えば、複数のコンテンツデータＣからなるアルバムを購入する形態で行ってもよい。この場合に、アルバムを構成する複数のコンテンツデータＣは、異なるコンテンツプロバイダ１０１によって提供されてもよい（後述する第２実施形態の場合には、さらに異なるサービスプロバイダ３１０によって提供されてもよい）。また、アルバムを構成する一部のコンテンツデータＣについての購入を行った後に、その他のコンテンツデータＣを追加する形で購入を行い、最終的にアルバムを構成する全てのコンテンツデータＣを購入してもよい。

【０１７９】図４１は、コンテンツデータＣの種々の購入形態の例を説明するための図である。図４１に示すように、ＡＶ機器１６０３は、ネットワーク機器１６０１がコンテンツプロバイダ１０１から受信したコンテンツデータＣを、権利書データ１０６を用いて購入し、利用制御データ１６６ａを生成している。また、ＡＶ機器１６０２は、ネットワーク機器１６０１がコンテンツプロバイダ１０１から受信したコンテンツデータＣを、権利書データ１０６を用いて購入し、利用制御データ１６６ｂを生成している。また、ＡＶ機器１６０３は、ＡＶ機器１６０２が購入したコンテンツデータＣを複製し、ＡＶ機器１６０２で作成した利用制御データ１６６ｂを用いて利用形態を決定している。これにより、ＡＶ機器１６０３において、利用制御データ１６６ｃが作成される。また、ＡＶ機器１６０３では、利用制御データ１６６ｃから利用履歴データ１０８ｂが作成される。また、ＡＶ機器１６０４は、ネットワーク機器１６０１がコンテンツプロバイダ１０１から受信して購入形態を決定したコンテンツデータＣを入力し、ネットワーク機器１６０１が作成した利用制御データ１６６を用いて当該コンテンツデータＣの購入形態を決定する。これにより、ＡＶ機器１６０４において、利用制御データ１６６$_{H}$が作成される。また、ＡＶ機器１６０４では、利用制御データ１６６ａから利用履歴データ１０８ａが作成される。なお、利用制御データ１６６ａ，１６６ｂ，１６６ｃは、ＡＶ機器１６０４，１６０２，１６０３において、それぞれ固有の記録用盤データ$_{SSTR}$，並びに記録メディア（媒体）に固有のメディア鍵データ$_{KMED}$を用いて暗号化され、記録媒体に記録される。本実施形態では、ユーザは、コンテンツデータＣの所有権に対して対価を支払うのではなく、使用権に対価を支払う。コンテンツデータの複製は、コンテンツのプロモーションに相当し、マーケットの拡販という観点からコンテンツデータ

64

の権利者の要請にかなう行為となる。

【０１８０】＜ＲＯＭ型の記録媒体のコンテンツデータの購入形態決定処理＞図４２に示すように、コンテンツの購入形態が未決定の図１１に示すＲＯＭ型の記録媒体１３０$_{1}$をユーザホームネットワーク３０３がオフラインで配給を受けた場合に、ＡＶ機器１６０$_{2}$において購入形態を決定する際の処理の流れを図４３および図４４を参照しながら説明する。図４４は、当該処理のフローチャートである。

ステップＳ４４－１：ＡＶ機器１６０$_{2}$のＳＡＭ１０５$_{2}$は、先ず、図４３に示す相互認証部１７０と図１１に示すＲＯＭ型の記録媒体１３０$_{1}$のメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ１３３からメディア鍵データ$_{KMED}$を入力する。なお、ＳＡＭ１０５$_{2}$が、事前にメディア鍵データ$_{KMED}$を保持している場合には、当該入力を行わなくても良い。

【０１８１】ステップＳ４４－２：ＲＯＭ型の記録媒体１３０$_{1}$のセキュアＲＡＭ領域１３２に記録されているセキュアコンテナ１０４に格納された図３（Ｂ）（Ｃ）に示すキーファイルＫＦおよびその署名データＳＩＧ$_{7.CP}$と、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1.ESC}$とを、メディア・ドライブＳＡＭ管理部８５５を介して入力して作業用メモリ２００に書き込む。

【０１８２】ステップＳ４４－３：署名処理部１８９において、署名データＳＩＧ$_{1.ESC}$の正当性を確認した後に、公開鍵証明書データＣＥＲ$_{CP}$から公開鍵データＫ$_{CP.P}$を取り出し、この公開鍵データＫ$_{CP.P}$を用いて、署名データＳＩＧ$_{7.CP}$の正当性、すなわちキーファイルＫＦの送信者の正当性を検証する。また、署名処理部１８９において、記憶部１９２から読み出した公開鍵データＫ$_{ESC.P}$を用いて、キーファイルＫＦに格納された署名データＳＩＧ$_{K1.ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性を検証する。

【０１８３】ステップＳ４４－４：署名処理部１８９において署名データＳＩＧ$_{7.CP}$，ＳＩＧ$_{K1.ESC}$の正当性が確認されると、作業用メモリ２００から暗号化・復号部１７２にキーファイルＫＦを読み出す。次に、暗号化・復号部１７２において、対応する端間のライセンス鍵データＫＤ$_{1}$～ＫＤ$_{3}$を用いて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_{1}$～ＳＤＣ$_{3}$を復号した後に、作業用メモリ２００に書き込む。

【０１８４】ステップＳ４４－５：図４３に示す相互認証部１７０と図４２に示すＡＶ圧縮・伸長用ＳＡＭ１６３との間で相互認証を行った後に、ＳＡＭ１０５$_{2}$のＡＶ圧縮・伸長用ＳＡＭ管理部１８４は、作業用メモリ２００Ｋに記憶されているコンテンツ鍵データＫｃおよび権利書データ１０６に格納された半間ボパラメータデータ

１９９、並びにＲＯＭ型の記録媒体１３０１のＲＯＭ領域１３１から読み出したコンテンツファイルＣＦに格納されたコンテンツデータＣを図４２に示すＡＶ圧縮・伸長用ＳＡＭ１６３において、コンテンツデータＣがコンテンツ鍵データＫｃを用いて半開示モードで復号された後に伸長され、再生モジュール２７０において、ＡＶ圧縮・伸長用ＳＡＭ１６３からのコンテンツデータＣが再生される。

【０１８５】ステップＳ４４－６：ユーザによる図４２に示す購入形態決定操作部１６５の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号Ｓ１６５が課金処理部１８７に入力される。

【０１８６】ステップＳ４４－７：課金処理部１８７は、操作信号Ｓ１６５に応じた利用制御データ１６６を作成し、これを作業用メモリ２００に書き込む。

ステップＳ４４－８：作業用メモリ２００から暗号化・復号部１７３に、コンテンツ鍵データＫｃおよび利用制御データ１６６が出力される。暗号化・復号部１７３は、作業用メモリ２００から入力したコンテンツ鍵データＫｃおよび利用制御データ１６６を、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入署鍵データK_{PUR}を用いて順次に暗号化して作識用メモリ２００に書き込む。

【０１８７】ステップＳ４４－９：メディアＳＡＭ管理部１９７において、作業用メモリ２００から読み出した、暗号化されたコンテンツ鍵データＫｃおよび利用制御データ１６６と、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$を用いて図３７（Ｃ）に示すキーファイルＫＦ$_1$が生成される。また、署名処理部１８９において、図３７（Ｃ）に示すキーファイルＫＦ$_1$のハッシュ値Ｈｋ$_1$が生成され、当該ハッシュ値Ｈｋ$_1$がメディア・ドライブＳＡＭ管理部８５５に出力される。

【０１８８】ステップＳ４４－１０：図４３に示す相互認証部１７０と図４２に示すメディアＳＡＭ１３３との間で相互認証を行った後に、メディア・ドライブＳＡＭ管理部８５５は、キーファイルＫＦ$_1$およびハッシュ値Ｈｋ$_1$を、図４２に示すメディア・ドラブＳＡＭ２６０を介してＲＯＭ型の記録媒体１３０１のセキュアＲＡＭ領域１３２に書き込む。これにより、購入形態が決定されたＲＯＭ型の記録媒体１３０１が得られる。このとき、課金処理部１８７が生成した利用制御データ１６６および利用履歴データ１０８は、所定のタイミングで、作業用メモリ２００および外部メモリ２０１からそれぞれ読み出しされたＥＭＤサービスセンタ１０２に送信される。なお、ＲＯＭ型の記録媒体１３０１のメディアＳＡＭ１３３にキーファイルＫＦが格納されている場合には、図４２において点線で示されるように、ＳＡＭ１０５$_2$はメディアＳＡＭ１３３からキーファイルＫＦを入力する。また、この場合に、ＳＡＭ１０５$_2$は、作成したキーファイルＫＦ$_1$をメディアＳＡＭ１３３に書き込む。

【０１８９】＜ＲＯＭ型の記録媒体のコンテンツデータの購入形態を決定した後に、ＲＡＭ型の記録媒体に書き込む場合の処理＞以下、図４５に示すように、ＡＶ機器１６０３において購入形態が未決定のＲＯＭ型の記録媒体１３０１からセキュアコンテナ１０４を読み出して新たなセキュアコンテナ１０４ｙを生成し、これをＡＶ機器１６０$_2$に転送し、ＡＶ機器１６０$_2$において購入形態を決定してＲＡＭ型の記録媒体１３０$_6$に書き込む際の処理の流れを図４６，図４７，図４８を参照しながら説明する。なお、ＲＯＭ型の記録媒体１３０１からＲＡＭ型の記録媒体１３０$_5$へのセキュアコンテナ１０４ｙの転送は、図１に示すネットワーク機器１６０１およびＡＶ機器１６０１～１６０$_4$のいずれの間で行ってもよい。図４８は、当該処理のフローチャートである。

【０１９０】ステップＳ４８－１：ＳＡＭ１０５$_3$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ１０５$_2$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ４８－２以降の処理を行う。また、ＳＡＭ１０５$_3$は、ＳＡＭ１０５$_2$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

ステップＳ４８－２：ＳＡＭ１０５$_3$とＳＡＭ１０５$_2$との間で相互認証が行われ、セッション鍵データK_{SES}が共有される。

【０１９１】ステップＳ４８－３：ＡＶ機器１６０$_3$のＳＡＭ１０５$_3$とＲＯＭ型の記録媒体１３０１のメディアＳＡＭ１３３との間で相互認証を行い、ＲＯＭ型の記録媒体１３０１のメディア鍵データK_{MED1}をＳＡＭ１０５$_3$に転送する。なお、メディア鍵データK_{MED1}を用いた暗号化をＲＯＭ型の記録媒体１３０１のメディアＳＡＭ１３３において行う場合には、メディア鍵データK_{MED1}の転送は行わない。

【０１９２】ステップＳ４８－４：ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$とＲＡＭ型の記録媒体１３０$_5$のメディアＳＡＭ１３３との間で相互認証を行い、ＲＡＭ型の記録媒体１３０$_5$のメディア鍵データK_{MED2}をＳＡＭ１０５$_2$に転送する。なお、メディア鍵データK_{MED2}を用いた暗号化をＲＡＭ型の記録媒体１３０$_5$のメディアＳＡＭ１３３において行う場合には、メディア鍵データK_{MED2}の転送は行わない。

【０１９３】ステップＳ４８－５：ＳＡＭ１０５$_3$は、図４６に示すように、メディア・ドライブＳＡＭ管理部８５５を介して、ＲＯＭ型の記録媒体１３０１のＲＯＭ領域１３１からコンテンツファイルＣＦおよびその署名データＳＩＧ$_{6.CF}$を読み出し、これをＳＡＭ管理部１９０に出力するとと共に、署名処理部１８９において、秘密鍵データ$K_{SAM3.5}$を用いて、これらの署名データＳＩＧ

$_{350,SAM3}$を作成する。

【０１９４】ステップＳ４８－６：ＳＡＭ１０５$_3$は、図４６に示すように、メディア・ドライブＳＡＭ管理部８５５を介して、ＲＯＭ型の記録媒体１３０$_1$のセキュアＲＡＭ領域１３２からキーファイルＫＦおよびその署名データＳＩＧ$_{7,CP}$を読み出し、これをＳＡＭ管理部１９０に出力すると共に、署名処理部１８９において、秘密鍵データＫ$_{SAM3,S}$を用いて、これらの署名データＳＩＧ$_{352,SAM3}$が作成される。

【０１９５】ステップＳ４８－７：ＳＡＭ１０５$_3$において、記憶部１９２からＳＡＭ管理部１９０に公開鍵証明書データＣＥＲ$_{SAM3}$およびその署名データＳＩＧ$_{351,ESC}$が読み出される。

【０１９６】ステップＳ４８－８：ＳＡＭ１０５$_3$の例えばＳＡＭ管理部１９０において、図４７に示すセキュアコンテナ１０４$_Y$が作成される。

【０１９７】ステップＳ４８－９：ＳＡＭ１０５$_3$の暗号化・復号部１７１において、ステップＳ４８－２で得たセッション鍵データＫ$_{SES}$を用いて、セキュアコンテナ１０４$_Y$が暗号化され、ＳＡＭ管理部１９０を介して、ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力される。

【０１９８】ステップＳ４８－１０：ＳＡＭ１０５$_2$では、図５０に示すように、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力した図４７に示すセキュアコンテナ１０４$_Y$が暗号化・復号部１７１においてセッション鍵データＫ$_{SES}$を用いて復号される。そして、当該復号されたセキュアコンテナ１０４$_Y$内のキーファイルＫＦおよびその署名データＳＩＧ$_{7,OP}$、ＳＩＧ$_{350,SAM3}$と、公開鍵証明書データＣＥＲ$_{SAM3}$およびその署名データＳＩＧ$_{351,ESC}$と、公開鍵証明書データＣＥＲ$_{ED}$およびその署名データＳＩＧ$_{1,ESC}$とが、作業用メモリ２００に書き込まれる。

【０１９９】ステップＳ４８－１２：ＳＡＭ１０５$_2$の署名処理部１８９において、セキュアコンテナ１０４$_Y$内に格納された署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{350,SAM3}$の正当性、すなわちコンテンツファイルＣＦの作成者および送信者の正当性を確認する。

ステップＳ４８－１３：コンテンツファイルＣＦの作成者および送信者が正当であると確認された後に、メディア・ドライブＳＡＭ管理部８５５を介してＲＡＭ型の記録媒体１３０$_S$のＲＡＭ領域１３４にコンテンツファイルＣＦが書き込まれる。

【０２００】ステップＳ４８－１４：署名処理部１８９において、署名データＳＩＧ$_{351,ESC}$が署名検証され、公開鍵証明書データＣＥＲ$_{SAM3}$の正当性が確認された後に、公開鍵証明書データＣＥＲ$_{SAM3}$に格納された公開鍵データＫ$_{SAM3}$および公開鍵データＫ$_{ESC,P}$を用いて、署名データＳＩＧ$_{7,CP}$，ＳＩＧ$_{352,SAM3}$，ＳＩＧ$_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者および送信者の正当性が検証される。

【０２０１】ステップＳ４８－１５：キーファイルＫＦの作成者および送信者の正当性が確認されると、作業用メモリ２００からキーファイルＫＦが読み出されて暗号化・復号部１７２に出力され、暗号化・復号部１７２において、ライセンス鍵データＫＤ$_i$（～ＫＤ$_3$）を用いて復号された後に、作業用メモリ２００に書き戻される。

【０２０２】ステップＳ４８－１６：作業用メモリ２００に記憶されている既に復号されたキーファイルＫＦに格納された権利書データ１０６が、利用監視部１８６に出力される。そして、利用監視部１８６において、権利書データ１０６に基づいて、コンテンツの購入形態および利用形態が管理（監視）される。

【０２０３】ステップＳ４８－１７：ユーザによる図３８に示す購入・利用形態決定操作部１６５の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。

ステップＳ４８－１８：課金処理部１８７において、決定された購入・利用形態に応じて利用制御データ１６６および利用履歴データ１０８が生成され、これが作業用メモリ２００および外部メモリ２０１にそれぞれ書き込まれる。利用制御データ１６６および利用履歴データ１０８は、所定のタイミングで、ＥＭＤサービスセンタ１０２に送信される。

【０２０４】ステップＳ４８－１９：コンテンツ鍵データＫｃおよび利用制御データ１６６が、作業用メモリ２００から暗号化・復号部１７３に読み出され、暗号化・復号部１７３において記憶部１９２から読み出した記録用鍵データＫ$_{ETR}$、メディア鍵データＫ$_{MED2}$および購入者鍵データＫ$_{PIN}$を用いて順に暗号化され、メディアＳＡＭ管理部１９７に出力される。また、作業用メモリ２００からメディアＳＡＭ管理部１９７に、キーファイルＫＦが出力される。

【０２０５】ステップＳ４８－２０：メディアＳＡＭ管理部１９７において、図３４（Ｃ）に示すキーファイルＫＦ$_i$が作成され、キーファイルＫＦ$_i$がメディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体１３０$_S$のメディアＳＡＭ１３３に書き込まれる。また、メディアＳＡＭ管理部１９７を介して、キーファイルＫＦがＲＡＭ型の記録媒体１３０$_S$のメディアＳＡＭ１３３に書き込まれる。

【０２０６】以下、ＳＡＭ１０５$_1$～１０５$_4$の実現方法について説明する。ＳＡＭ１０５$_1$～１０５$_4$の機能をハードウェアとして実現する場合は、メモリを内蔵したＡＳＩＣ型のＣＰＵを用いて、そのメモリには、図２２に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテ

ンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【０２０７】例えば、図２２に示す暗号化・復号部１７１などのモジュールは、例えば、処理速度の問題でハードウエアとしてＡＳＩＣ型のＣＰＵ内のＩＰコアとして実装される。クロック速度やＣＰＵコード体系などの性能によっては、暗号化・復号部１７１をソフトウェアとして実装してもよい。また、図２２に示す記憶部１９２や、図２２に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシュＲＯＭ）が用いられ、作業用メモリとしてはＳＲＡＭなどの高速書き込み可能なメモリが用いられる。なお、その他にも、ＳＡＭ１０５１～１０５４に内蔵されるメモリとして、強誘電体メモリー（ＦｅＲＡＭ）を用いてもよい。また、ＳＡＭ１０５１～１０５４には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【０２０８】上述したように、ＳＡＭ１０５1～１０５4は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。ＳＡＭ１０５1～１０５4を搭載した機器のホストＣＰＵのバス経由で、当該ＳＡＭのＩＣ内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、ＳＡＭのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、頻繁に書き込まれたりしないように、すなわち、搭載機器のホストＣＰＵが割り付けているアドレス空間内に存在しないように、当該ＳＡＭでは、ＣＰＵ側のメモリー空間を管理するＭＭＵ(Memory Magagement Unit)を用いて、搭載機器側のホストＣＰＵからは見えないアドレス空間を設定する。また、ＳＡＭ１０５1～１０５4は、Ｘ線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウエアＩＣＥ、ソフトウエアＩＣＥ）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがＩＣ製造後には使用できないような構造をしている。ＳＡＭ１０５1～１０５4自身は、ハードウエア的な構造においては、メモリを内蔵した通常のＡＳＩＣ型のＣＰＵであり、機能は当該ＣＰＵを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なＡＳＩＣ型のＣＰＵと異なる。

【０２０９】ＳＡＭ１０５1～１０５4の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理をおこなう場合と、通常のセットに搭載されているホストＣＰＵ上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがＩＰコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタンスソフトウェアと呼ばれるもので、ＩＣＥ（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（ＭｉｎｉＯＳ）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【０２１０】次に、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３について説明する。図２２に示すように、ＡＶ圧縮・伸長用ＳＡＭ１６３は、相互認証部２２０、復号部２２１、復号部２２２、伸長部２２３、電子透かし情報処理部２２４および半開示処理部２２５を有する。相互認証部２２０は、ＡＶ圧縮・伸長用ＳＡＭ１６３がＳＡＭ１０５１からデータを入力する際に、図２３に示す相互認証部１７０との間で相互認証を行ってセッション鍵データＫｓｅｓを生成する。

【０２１１】復号部２２１は、ＳＡＭ１０５1から入力したコンテンツ鍵データＫｃ、半開示パラメータデータ１９９、ユーザ電子透かし情報用データ１９６およびコンテンツデータＣを、セッション鍵データＫｓｅｓを用いて復号する。そして、復号部２２１は、復号したコンテンツ鍵データＫｃおよびコンテンツデータＣを復号部２２２に出力し、復号したユーザ電子透かし情報用データ１９６を電子透かし情報処理部２２４に出力し、半開示パラメータデータ１９９を半開示処理部２２５に出力する。

【０２１２】復号部２２２は、半開示処理部２２５からの制御に基づいて、コンテンツ鍵データＫｃを用いて、コンテンツデータＣを半開示状態で復号し、復号したコンテンツデータＣを伸長部２２３に出力する。

【０２１３】伸長部２２３は、復号されたコンテンツデータＣを伸長して、電子透かし情報処理部２２４に出力する。伸長部２２３は、例えば、図３（Ａ）に示すコンテンツファイルＣＦに格納されたＡ／Ｖ伸長用ソフトウェアを用いて伸長処理を行い、例えば、ＡＴＲＡＣ３方式で伸長処理を行う。

【０２１４】電子透かし情報処理部２２４は、復号されたユーザ電子透かし情報用データ１９６に応じたユーザ電子透かし情報を、復号された前記コンテンツデータＣに埋め込み、新たなコンテンツデータＣを生成する。電子透かし情報処理部２２４は、当該新たなコンテンツデータ

Ｃを再生モジュール１６９に出力する。このように、ユーザ電子透かし情報は、コンテンツデータＣを再生するときに、ＡＶ圧縮・伸長用ＳＡＭ１６３において埋め込まれる。なお、本発明では、コンテンツデータＣにユーザ電子透かし情報用データ１９６を埋め込まないようにしてもよい。

【０２１５】半導体処理部２２５は、半導体パラメータデータ１９９に基づいて、例えば、コンテンツデータＣのうち復号を行わないブロックと、復号を行うブロックとを復号部２２２に指示する。また、半導体処理部２２５は、その他に、半導体パラメータデータ１９９に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【０２１６】再生モジュール１６９は、復号および伸長されたコンテンツデータＣに応じた再生を行う。

【０２１７】次に、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。図５１（Ａ）は、コンテンツプロバイダ１０１からＳＡＭ１０５１にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５１に、コンテンツプロバイダ１０１とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod_{50}が送信される。モジュールMod_{50}には、モジュールMod_{51}およびその秘密鍵データ$K_{EP,S}$による署名データSIG_{EP}が格納されている。モジュールMod_{51}には、コンテンツプロバイダ１０１の秘密鍵データ$K_{EP,P}$を格納した公開鍵証明書データCER_{EP}と、公開鍵証明書データCER_{EP}に対しての秘密鍵データ$K_{ESG,S}$による署名データＳＩＧ$_{ESG}$と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データCER_{EP}を格納したモジュールMod_{50}を、コンテンツプロバイダ１０１からＳＡＭ１０５１に送信することで、ＳＡＭ１０５１において署名データＳＩＧ$_{EP}$の検証を行なう際に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に公開鍵証明書データCER_{EP}を送信する必要がなくなる。

【０２１８】図５１（Ｂ），（Ｃ）は、コンテンツプロバイダ１０１からＳＡＭ１０５１にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５１に、コンテンツプロバイダ１０１とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５１（Ｂ）に示すモジュールMod_{52}が送信される。モジュールMod_{52}には、送信するデータＤａｔａと、その秘密鍵データ$K_{EP,S}$による署名データＳＩＧ$_{EP}$とが格納されている。また、ＥＭＤサービスセンタ１０２からＳＡＭ１０５１には、ＥＭＤサービスセンタ１０２とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５１（Ｃ）に示すモジュールMod_{53}が送信される。モジュールMod_{53}には、コンテンツプロバイダ１０１の公開鍵証明書データCER_{EP}と、その秘密鍵データ$K_{ESG,S}$による署名データＳＩＧ$_{ESG}$とが格納されている。

【０２１９】図５１（Ｄ）は、ＳＡＭ１０５１からコンテンツプロバイダ１０１にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５１からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod_{54}が送信される。モジュールMod_{54}には、モジュールMod_{55}およびその秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$が格納されている。モジュールMod_{55}には、ＳＡＭ１０５１の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データ$K_{ESG,S}$による署名データＳＩＧ$_{ESG}$と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データCER_{SAM1}を格納したモジュールMod_{55}を、ＳＡＭ１０５１からコンテンツプロバイダ１０１に送信することで、コンテンツプロバイダ１０１において署名データＳＩＧ$_{SAM1}$の検証を行なう際に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に公開鍵証明書データCER_{SAM1}を送信する必要がなくなる。

【０２２０】図５１（Ｅ），（Ｆ）は、ＳＡＭ１０５１からコンテンツプロバイダ１０１にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５１からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５１（Ｅ）に示すモジュールMod_{56}が送信される。モジュールMod_{56}には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$とが格納されている。また、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１には、ＥＭＤサービスセンタ１０２とコンテンツプロバイダ１０１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５１（Ｆ）に示すモジュールMod_{57}が送信される。モジュールMod_{57}には、ＳＡＭ１０５１の公開鍵証明書データCER_{SAM1}と、その秘密鍵データ$K_{ESG,S}$による署名データＳＩＧ$_{ESG}$とが格納されている。

【０２２１】図５２（Ｇ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａ

をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ５８が送信される。モジュールＭｏｄ５８には、モジュールＭｏｄ５９およびその秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}が格納されている。モジュールＭｏｄ５８には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。

【０２２２】図５２（Ｈ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５２（Ｈ）に示すモジュールＭｏｄ６０が送信される。モジュールＭｏｄ６０には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}とが格納されている。このとき、ＥＭＤサービスセンタ１０２にはコンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}は既に登録されている。

【０２２３】図５２（Ｉ）は、ＳＡＭ１０５１からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５１からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ６１が送信される。モジュールＭｏｄ６１には、モジュールＭｏｄ６２およびその秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}が格納されている。モジュールＭｏｄ６２には、ＳＡＭ１０５１の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。

【０２２４】図５２（Ｊ）は、ＳＡＭ１０５１からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５１からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図５２（Ｊ）に示すモジュールＭｏｄ６３が送信される。モジュールＭｏｄ６３には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}とが格納されている。このとき、ＥＭＤサービスセンタ１０２にはＳＡＭ１０５１の公開鍵証明書データCER_{SAM1}は既に登録されている。

【０２２５】以下、ＳＡＭ１０５１～１０５４の出荷時におけるＥＭＤサービスセンタ１０２への登録処理について説明する。なお、ＳＡＭ１０５１～１０５４の登録処理は同じであるため、以下、ＳＡＭ１０５１の登録処理について述べる。ＳＡＭ１０５１の出荷時には、ＥＭＤサービスセンタ１０２の鍵サーバ１４１によって、ＳＡＭ管理部１４９を介して、図２３などに示す記憶部１９２に以下に示す鍵データが初期登録される。また、ＳＡＭ１０５１には、例えば、出荷時に、記憶部１９２などに、ＳＡＭ１０５１がＥＭＤサービスセンタ１０２に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部１９２には、例えば、図２７において左側に「＊」が付されているＳＡＭ１０５１の識別子ＳＡＭ＿ＩＤ、記録用鍵データK_{STR}、ルート認証局２の公開鍵データK_{R-CA}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ１０５１の秘密鍵データ$K_{SAM1,S}$、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$、ＡＶ圧縮・伸長用ＳＡＭ１６３およびメディアＳＡＭとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データCER_{SAM1}は、ＳＡＭ１０５１を出荷後に登録する際にＥＭＤサービスセンタ１０２からＳＡＭ１０５１に送信してもよい。

【０２２６】また、記憶部１９２には、ＳＡＭ１０５１の出荷時に、図３に示すコンテンツファイルＣＦおよびキーファイルＫＦを読み込み形式を示すファイルリーダが、ＥＭＤサービスセンタ１０２によって書き込まれる。ＳＡＭ１０５１では、コンテンツファイルＣＦおよびキーファイルＫＦに格納されたデータを利用する際に、記憶部１９２に記憶されたファイルリーダが用いられる。

【０２２７】ここで、ルート認証局２の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているＲＳＡを使用し、データ長は例えば１０２４ビットである。公開鍵データK_{CR-CA}は、図１に示すルート認証局２によって発行される。また、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$は、短いデータ長でＲＳＡと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば１６０ビットである。但し、暗号化の強度を考慮すると、公開鍵データ$K_{ESC,P}$は１９２ビット以上であることが望ましい。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２に公開鍵データ$K_{ESC,P}$を登録する。また、ルート認証局９２は、公開鍵データ$K_{ESC,P}$の公開鍵証明

75

書データＣＥＲesc を作成する。公開鍵データKesc,P を格納した公開鍵証明書データＣＥＲesc は、好ましく、ＳＡＭ１０５１の出荷時に記憶部１９２に記憶される。この場合に、公開鍵証明書データＣＥＲesc は、ルート認証局９２の秘密鍵データKROOT,S で署名されている。

【０２２８】ＥＭＤサービスセンタ１０２は、乱数を発生してＳＡＭ１０５１の秘密鍵データKSAM1,S、を生成し、これとペアとなる公開鍵データKSAM1,P を生成する。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２の認証をももって、公開鍵データKSAM1,P の公開鍵証明書データＣＥＲSAM1 を発行し、これに自らの秘密鍵データKESC,S を用いて署名データを添付する。すなわち、ＥＭＤサービスセンタ１０２は、セカンドＣＡ（認証局）として機能を果たす。

【０２２９】また、ＳＡＭ１０５１には、ＥＭＤサービスセンタ１０２により、ＥＭＤサービスセンタ１０２の管理下にある一意（ユニーク）な識別子ＳＡＭ＿ＩＤが割り当てられ、これがＳＡＭ１０５１の記憶部１９２に格納されると共に、ＥＭＤサービスセンタ１０２によって管理される。

【０２３０】また、ＳＡＭ１０５１は、出荷後、例えば、ユーザによってＥＭＤサービスセンタ１０２と接続され、登録手続を行うと共に、ＥＭＤサービスセンタ１０２から記憶部１９２にライセンス鍵データＫＤ１～ＫＤ３が転送される。すなわち、ＳＡＭ１０５１を利用するユーザは、コンテンツをダウンロードする前にＥＭＤサービスセンタ１０２に登録手続が必要である。この登録手続は、例えば、ＳＡＭ１０５１を搭載している機器（当該例では、ネットワーク機器１６０１）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報（ユーザの氏名、住所、連絡先、性別、決済口座、ログイン名、パスワードなど）を記載して例えば郵便などのオフラインで行なわれる。ＳＡＭ１０５１は、上述した登録手続を経た後でないと使用できない。

【０２３１】ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５１のユーザによる登録手続に応じて、ユーザに固有の識別子ＵＳＥＲ＿ＩＤを発行し、例えば、ＳＡＭ＿ＩＤとＵＳＥＲ＿ＩＤとの対応関係を管理し、課金時に利用する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５１のユーザに対して情報参照用識別子ＩＤと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子ＩＤとパスワードとを用いて、ＥＭＤサービスセンタ１０２に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、ＥＭＤサービスセンタ１０２は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

76

【０２３２】次に、図２７に示すように、ＳＡＭ１０５１内の記憶部１９２にＳＡＭ登録リストを格納する手順について説明する。図１に示すＳＡＭ１０５１は、例えば、バス１９１としてＩＥＥＥ１３９４シリアルバスを用いた場合に、バス１９１に接続された機器の電源を立ち上げたり、新しい機器をバス１９１に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するＳＡＭ１０５２～ＳＡＭ１０５４のＳＡＭ登録リストを得る。なお、ＩＥＥＥ１３９４シリアルバスであるバス１９１に応じて生成されたトポロジーマップは、例えば、図５３に示すように、バス１９１にＳＡＭ１０５１～１０５４に加えてＡＶ機器１６０ｓ，１６０ｔのＳＣＭＳ処理回路１０５ｓ，１０５ｔが接続されている場合に、ＳＡＭ１０５１～１０５４およびＳＣＭＳ処理回路１０５ｓ，１０５ｔを対象として生成される。従って、ＳＡＭ１０５１は、当該トポロジーマップから、ＳＡＭ１０５１～１０５４についての情報を抽出して図５４に示すＳＡＭ登録リストを生成する。

【０２３３】そして、ＳＡＭ１０５１は、図５４に示すＳＡＭ登録リストを、ＥＭＤサービスセンタ１０２に登録して署名を得る。これらの処理は、バス１９１のセッションを利用してＳＡＭ１０５１が自動的に行い、ＥＭＤサービスセンタ１０２にＳＡＭ登録リストの登録命令を発行する。ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５１から図５４に示すＳＡＭ登録リストを受けると、有効期限を確認する。そして、ＥＭＤサービスセンタ１０２は、登録時にＳＡＭ１０５１より指定された決済機能の有無を参照して対応する部分の設定を行う。また、ＥＭＤサービスセンタ１０２は、予め保持している図５５に示すリポケーションリストＣＲＬをチェックしてＳＡＭ登録リスト内のリポケーションフラグを設定する。リポケーションリストは、例えば、不正使用などを理由にＥＭＤサービスセンタ１０２によって使用が禁止されている（無効な）ＳＡＭのリストである。各ＳＡＭは他のＳＡＭと通信を行う際に、リポケーションリストによって通信相手のＳＡＭが無効にされている場合には、当該通信相手のＳＡＭとの通信を停止する。また、ＥＭＤサービスセンタ１０２は、決済時にはＳＡＭ１０５１に対応するＳＡＭ登録リストを取り出し、その中に記述されたＳＡＭがリポケーションリストに含まれているかを確認する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ登録リストに署名を添付する。これにより、図５６に示すＳＡＭ登録リストが作成される。なお、ＳＡＭリポケーションリストは、同一系の（同一のバス１９１に接続されている）ＳＡＭのみを対象として生成され、各ＳＡＭに対応するリポケーションフラグによって、当該ＳＡＭの有効および無効を示している。

【０２３４】なお、リポケーションリストＣＲＬの更新は、例えば、ＥＭＤサービスセンタ１０２からＳＡＭに放送される更新データに応じて、ＳＡＭ内部で自動的に

行なうことが好ましい。

【０２３５】以下、ＳＡＭが持つセキュリティ機能について説明する。ＳＡＭは、セキュリティに関する機能として、共通鍵暗号方式のＤＥＳ（Triple DES/AES）、公開鍵暗号方式の楕円曲線暗号（署名生成／検証ＥＣ－ＤＳＡ，共有鍵生成ＥＣ－Ｄ．Ｈ．，公開鍵暗号ＥＣ－ElGamal），圧縮関数のハッシュ関数ＳＨＡ－１，乱数生成器（真性乱数）の暗号ライブラリーのＩＰ部品を有している。相互認証、署名生成、署名検証、共有鍵（セッション鍵）作成（配送）には公開鍵暗号方式（楕円曲線暗号）が用いられ、コンテンツの暗号、復号には共通鍵暗号（ＤＥＳ）が用いられ、署名生成、検証の中のメッセージ認証に圧縮関数（ハッシュ関数）が用いられる。

【０２３６】図５７は、ＳＡＭが持つセキュリティ機能を説明するための図である。ＳＡＭが管理するセキュリティー機能は、コンテンツに関連する暗号、復号処理をつかさどるアプリケーション層でのセキュリティー機能（１）と、通信相手と相互認証をしてセキュアな通信路を確保する物理層のセキュリティー機能（２）との２種類がある。ＥＭＤシステム１００では、配信されるコンテンツデータＣはすべて暗号化され、決済と同時に鍵の購入手続きをすることを前提としている。権利書データ１０６は、コンテンツデータＣと一緒にイン・バンド方式で送られることを前提としているので、ネットワークの媒体と関係のない層でそのデータが管理され、衛星、地上波、ケーブル、無線、記録媒体（メディア）などの流通経路によらず、共通な複利処理システムを提供できる。具体的には、権利書データ１０６をネットワークの物理層のプロトコルのヘッダに挿入したりすると、使用するネットワークによって、挿入するデータが同じでも、ヘッダのどこに挿入するかを各々のネットワークで決めないといけない。

【０２３７】本実施形態では、コンテンツデータＣおよびキーファイルＫＦの暗号化は、アプリケーション層での保護を意味している。相互認証は、物理層やトランスポート層で行ってもよいし、アプリケーション層で行ってもよい。物理層に暗号機能を組み込むことは、使用するハードウエアに暗号機能を組み込むことを意味している。送信、受信の両者間のセキュアの通信路を確保することが相互認証の本来の目的なので物理層で実現できることが望ましいが、実際はトランスポート層で実現し、伝送路によらないレベルでの相互認証が多い。

【０２３８】ＳＡＭが実現するセキュリティ機能には、通信先の相手の正当性を確認するための相互認証と、アプリケーション層での調金処理をともなうコンテンツデータの暗号化および復号とがある。機器間で通信を行う際のＳＡＭ相互間での相互認証は、通常、アプリケーション層レベルに実装されるが、トランスポート層や物理層などの他のレイヤに実装されてもよい。物理層に実装する相互認証は、５Ｃ１３９４ＣＰ（Content Protection）を利用する。１３９４ＣＰは１３９４ＬＩＮＫＩＣ（ハードウエア）のIsochronousChanneｌ に共通鍵暗号であるＭ６がＳ実装されており、Asynchronous Channelによる相互認証（楕円曲線暗号、ハッシュ関数を利用した共通鍵暗号）の結果、生成されるセッション鍵をIsochronous Channel のＭ６に転送し、Ｍ６による共通鍵暗号を実現する。

【０２３９】ＳＡＭ相互間の相互認証を物理層のハードウエア上に実装する場合には、公開鍵暗号（楕円曲線暗号）を利用した相互認証で生成されたセッション鍵をホストＣＰＵを介して１３９４ＬＩＮＫＩＣのＭ６に転送し、１３９４ＣＰで生成されたセッション鍵と併用してコンテンツデータの暗号化を行う。また、ＳＡＭ相互間の相互認証をアプリケーション層で行う場合には、ＳＡＭ内部の共通鍵暗号ライブラリ（DES/Triple DES/AES)を使って暗号化を行う。

【０２４０】本実施形態では、例えば，ＳＡＭ相互間の相互認証をアプリケーション層に実装し、１３９４ＣＰによる相互認証を１３９４ＬＩＮＫＩＣという物理層（ハードウエア）に実装する。この場合に、課金処理をともなうコンテンツデータの暗号化および復号はアプリケーション層でおこなわれるが、アプリケーション層は一般ユーザから簡単にアクセスでき、時間無制限に解析される可能性があるため、当該課金処理をともなう処理に関しては、本実施形態では、外部からも処理内容をいっさいモニタ（監視）できない耐タンパ性をもったハードウエア内部で行っている。これがＳＡＭを耐タンパ性の構造を持ったハードウエアで実現する最大の理由である。なお、当該課金処理をホストＣＰＵ内で行う場合は、ＣＰＵに耐タンパ性のソフトウェアを実装する。

【０２４１】図５８は、コンテンツプロバイダ１０１からネットワーク機器１６０に送信されたセキュアコンテナ１０４に格納されたコンテンツデータＣをＡＶ機器（ストレージ機器）１６０において記録媒体（メディア）に書き込む際に行われる、コンテンツプロバイダ１０１およびＳＡＭ１０５におけるセキュリティ機能を説明するための図である。コンテンツプロバイダ１０１からネットワーク機器１６０に送信されるセキュアコンテナ１０４内のコンテンツデータＣは、コンテンツプロバイダ１０１が管理しているコンテンツ鍵データＫｃで暗号化されている。コンテンツ鍵データＫｃおよび権利書データ１０６は、ＥＭＤサービスセンタ１０２が管理するライセンス鍵データＫＤで暗号化されている。図５８に示す例では、セキュアコンテナ１０４が、ネットワークの物理層のプロトコルでカプセル化され、クライアントのネットワーク機器１６０にダウンロードされる。その過程で、コンテンツプロバイダ１０１およびＳＡＭ１０５において乱数を生成し、公開鍵暗号方式と共通鍵暗号方式とを併用して相互認証をおこなう。そして、ネットワーク機器１６０において、ダウンロード

されたセキュアコンテナ１０４が、メディアに記録される。このとき、購入形態が決定され、コンテンツ鍵データＫｃおよび権利書データ１０６がライセンス鍵データＫＤを用いて暗号化された後にメディアに記録され、利用制御データ１６６がメディア鍵データK_{MED}および記録用鍵データK_{STR}を用いて暗号化された後にメディアに記録される。

【０２４２】図５９（Ａ）は一般的に用いられるＯＳＩ参照モデルにおける送信側および受信側の各層（レイヤー）で行われる通信を説明するための図、図５９（Ｂ）は図５８に示すコンテンツプロバイダ１０１とネットワーク機器１６０１（ＳＡＭ１０５１）との間での通信時の保護機能を詳細に説明するための図である。図５９（Ａ）に示すように、ＯＳＩ参照モデルでは、送信側および受信側において物理層、データリンク層、トランスポート層、・・・、ソケット層およびアプリケーション層が下から上に順に構築され、対応するレイア相互間でデータのやりとりが行われる。また、コンテンツプロバイダ１０１とネットワーク機器１６０１（ＳＡＭ１０５１）との間の通信は、図５９（Ｂ）に示す階層構造に基づいて行われる。図５９（Ｂ）に示す例では、物理層としてＨＤＬＣ，Ｖ．２３および／またはＸ．２５などが用いられ、トランスポート層としてＩＰなどが用いられ、ソケット層としてＳｏｃｋｅｔ（ＡＰＩ）などが用いられ、アプリケーション層としてｈｔｔｐ，ＸＭＬ／ＳＭＩＬ／ＨＴＭＬなどが用いられ、各層が独自のセキュリティ機能を有している。

【０２４３】ここで、物理層では伝送路上の保護が行われ、当該伝送路を伝送するアプリケーションに関するデータを保護できる。当該物理層での保護は、ハードウエアでの保護機能の実装が前提になる。トランスポート層での保護は、伝送路には依存しないが、トランスポートプロトコルを使用している全てのアプリケーションに関するデータについて行われる。ソケット層での保護は、当該ソケットを利用しているアプリケーションに関する全てのデータについて行われる。アプリケーション層での保護は、全てのアプリケーションに関するデータを保護することができるが、一般ユーザによる解析、改竄の可能性が高い。

【０２４４】ネットワーク経由の処理には、すくなくとも２つのプログラムが存在する。一つはローカルにあるプラットフォーム上で動くプログラムで、ユーザが操作する。もう一つはサービスを提供するプログラム（アプリケーション）で、ネットワークを介した通信先にある（リモート）プラットフォーム上で動くものである。図５９（Ａ），（Ｂ）に示すように、各レイヤーがお互いの上下の要素とやりとりすることにより、結果的に通信が可能になる。下側の要素との間で受け渡される情報は、対応するレベルの要素と直接やりとりしている、とみることができる。つまり、送信側の物理層は、受信側の物理層と、送信側のアプリケーションは、受信側のアプリケーションと通信しているようにみえる。

【０２４５】送信、受信の間で情報を保護するには、図５９（Ａ），（Ｂ）に示すように、直接やりとりするレイヤー間で保護する仕組みを作ればよい。これは送信側のあるレイヤーで情報を暗号化することは、受信側の対応するレイヤーでないと復号できないことを意味する。その場合、アプリケーション層、トランスポート層、データリンク層、・・・、物理層の各レイヤーで暗号化して保護する。物理層での保護は、ハードウエアレベルでの保護になる。ネットワークでは伝送路のハードウエアに依存するところを暗号化する。パケッシージでは記録媒体（メディア）に関与するハードウエア部に絡んだ部分を暗号する。データリンク層（ＭＡＣ層）は、比較的物理層に依存しているレイヤーなので物理層での保護の箝噛に入れる。トランスポート層は、ＴＣＰ／ＩＰのＩＰパケットレベルでの保護になる。これはＩＰパケットでの保護機能であるＩＰ Secが有名である。この方式の場合は、相手も同じ機構（ＩＰ Sec）を用意していれば、パケットに含まれるすべての情報が保護できる。ただし、パケットレベルでの処理にはカーネルの再構築が必要である。ソケットレベルでの保護には、例えば、ＳＳＬ（Secure Socket Layer）が用いられる。Socket ＡＰＩはＴＣＰ／ＩＰ関連のアプリケーションソフトを書くとき、このソケットを利用して書くための一種のＡＰＩ層で、このレベルでの保護は、そのソケットを利用するすべてのアプリケーションを保護できることを意味している。逆にそのソケットを利用しないアプリケーションは保護できない。最後にアプリケーションレベルでの保護は、アプリケーションの内部でデータを保護する方式である。これを利用すれば伝送路に依存せず、すべてのアプリケーションを保護することができる。

【０２４６】アプリケーションレベルで保護するプログラムは、カーネルを再構築する必要がなく、簡単にシステムを構築できるため、頻繁に使用される。そうすると、すべてアプリケーション層でデータを暗号化すれば、簡単で問題ないように思われるがアプリケーション層は一般ユーザが唯一操作できるレイヤーで、時間無制限にハッカー（暗号解読）できるチャンスがある。逆にカーネル、あるいはハードウエアに依存した暗号化は、一般ユーザから操作できない部分であり、この部分に依存した暗号化は非常に強固である。カーネル、ハードウエアに依存したレイヤーでの暗号化は、送信、受信間で、両方ともその暗号化に対応するシステムでないと成立しない。

【０２４７】図６０は、図５８に示すネットワーク機器１６０１（ＳＡＭ１０５１）とＡＶ機器１６０２（ＳＡＭ１０５２）との間の通信時の保護機能を詳細に説明するための図である。図６０に示すように、ＡＶ機器１６０２（ＳＡＭ１０５２）では、物理層としてセクタおよ

びファイルシステムが用いられ、トランスポート層としてＩＰが用いられ、トランスポート層とアプリケーション層の間にＨＡＶｉなどのホームネットワークミドルウェアが用いられている。ここで、物理層（セクタ）からアプリケーション層までの全ての層の通信データは記録媒体（メディア）に記録される際にメディア鍵データK_{MED}を用いて暗号化されていることで保護され、ファイルシステムからアプリケーション層までの全ての層の通信データは記録媒体に記録される際に記録用鍵データK_{STR}を用いて暗号化されて保護される。

【０２４８】ネットワーク機器１６０$_1$が受信したコンテンツデータを、ＡＶ機器１６０$_2$において記録媒体（メディア）に記録する場合には、ハードウェアと記録媒体という物理層でのセキュリティ保護が必要になる。このような物理層でのセキュリティ保護を実現するために、本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}の２種類を鍵データを定義する。記録用鍵データK_{STR}は、機器の種類ごとに定義されている鍵でセクタレベルの物理層を除いたアプリケーション層からトランスポート層まで、どのレイヤーで暗号化してもよい。記録用鍵データK_{STR}はＳＡＭ内に格納されており、ＳＡＭ内で記録用鍵データK_{STR}を用いた暗号化および復号が行なわれる。

【０２４９】メディア鍵データK_{MED}は、各記録媒体に定義されている鍵で、個々の記録媒体毎に定義および記録されている。メディア鍵データK_{MED}を用いた暗号化は、どのレイヤーで行なってもよいが、記録媒体という物理層レベルでの保護が前提の鍵なので、記録媒体の物理層に依存した部分に実装するのがより良い。例えば、記録媒体上に暗号化および復号を行なうメディアＳＡＭがあり、当該メディアＳＡＭにおいて暗号化および復号することが望ましい。あるいは、機器側の記録媒体の物理層に関連する信号処理部分にハードウエアとして実装し、そこにメディア鍵データを記録媒体から転送して（相互認証が必要）、暗号化および復号を行なってもよい。記録媒体のの物理層に依存しない部分で暗号化および復号を行なうには、ＳＡＭと相互認証をして、生成されたセッション鍵データK_{SES}でメディア鍵データK_{MED}を暗号化して機器側のＳＡＭに転送し、そこで暗号および復号を行なってもよい。これは、鍵の定義のみで、メディア上という物理層レベルを保護していることになる。

【０２５０】図６１は、例えば、図１に示すＡＶ機器１６０$_2$において図１１に示すＲＯＭ型の記録媒体１３０$_1$からコンテンツデータＣを再生し、当該再生したコンテンツデータをバス１９１を介してＡＶ機器１６０$_3$に伝送し、ＡＶ機器１６０$_3$において図１４に示すＲＡＭ型の記録媒体１３０$_4$に記録する場合のセキュリティ処理を説明するための図である。以下に示す（Ａ）～（Ｍ）は、当該処理の手順を示し、図６１に示された符号と対応している。

【０２５１】（Ａ）：再生側のＡＶ機器１６０$_2$とＲＯＭ型の記録媒体１３０$_1$のメディアＳＡＭ１３３$_1$との間で相互認証を行う。

（Ｂ）：記録側のＡＶ機器１６０$_3$とＲＡＭ型の記録媒体１３０$_4$のメディアＳＡＭ１３３$_4$との間で相互認証を行う。のメディア（Media-ＳＡＭ）とＳＡＭとで相互認証。

（Ｃ），（Ｄ）：ＡＶ機器１６０$_2$とＡＶ機器１６０$_3$との間で１３９４シリアルバスの機能を用いた相互認証（機器間認証）を行い、両者でセッション鍵データK_{SES}を共有する。

（Ｅ），（Ｆ）：上記（Ａ），（Ｂ）の認証結果を使用して、ＳＡＭ１０５$_2$とＳＡＭ１０５$_3$との間の相互認証（End to End 認証）を行い、セッション鍵が共有される

【０２５２】（Ｇ）：メディアＳＡＭ１３３$_1$あるいはＳＡＭ１０５$_2$によって、ＲＯＭ領域１３１から読み出されたコンテンツファイルＣＦおよびキーファイルＫＦが、メディア鍵データK_{MED2}を用いて復号（開錠）される。

（Ｈ）：ＳＡＭ１０５$_2$によって、コンテンツファイルＣＦおよびキーファイルＫＦが、記録用鍵データK_{STR2}を用いて復号される。

（Ｉ）：ＳＡＭ１０５$_2$において、コンテンツファイルＣＦに格納されたコンテンツデータの再生、記録に伴う署名検証および購入形態決定処理などの権利処理が行われる。なお、コンテンツデータＣの再生時には、コンテンツ鍵データＫｃによる復号処理が行われる。

（Ｊ）：コンテンツファイルＣＦおよびキーファイルＫＦが、ＡＶ機器１６０$_2$において上記（Ｅ），（Ｆ）および（Ｃ），（Ｄ）で生成されたセッション鍵データK_{SES}を用いて暗号化され、ＡＶ機器１６０$_3$に送信され、ＡＶ機器１６０$_3$において同じセッション鍵データK_{SES}を用いて復号される。

【０２５３】（Ｋ）：ＳＡＭ１０５$_2$で権利処理が行なわれていない場合には、ＳＡＭ１０５$_3$で権利処理が行なわれる。

（Ｌ）：ＳＡＭ１０５$_3$において、コンテンツファイルＣＦおよびキーファイルＫＦが、記録用鍵データK_{STR2}を用いて暗号化される。

（Ｍ）：ＳＡＭ１０５$_3$あるいはメディアＳＡＭ１３３$_4$において、コンテンツファイルＣＦおよびキーファイルＫＦが、メディア鍵データK_{MED}を用いて暗号化され、ＲＡＭ型の記録媒体１３０$_4$のＲＡＭ領域１３４に記録される。

【０２５４】以下、図１に示すユーザホームネットワーク１０３内の例えばネットワーク機器１６０$_1$内での各種のＳＡＭに搭載形態の一例を図６２を参照しながら説明する。図６２に示すように、ネットワーク機器１６０

１内には、ホストＣＰＵ８１０１、ＳＡＭ１０５１、ダウンロードメモリ１６７、メディア・ドラブＳＡＭ２６０、ドライブＣＰＵ１００３、ＤＲＡＭなどのショックプルーフ(Shock Proof)メモリ１００４を有する。ダウンロードメモリ１６７と、ショックプルーフメモリ１００４の一部の記憶領域は、ＳＡＭ１０５１およびホストＣＰＵ８１０１の双方からアクセス可能な共有メモリとして用いられる。ダウンロードメモリ１６７は、メモリコントローラ、バスアービターおよびブリッジの機能を持つモジュール１００５を介して、ホストＣＰＵバス１０００に接続されている。ダウンロードメモリ１６７およびショックプルーフメモリ１００４には、前述したコンテンツファイルＣＦおよびキーファイルＫＦなどが記憶される。ショックプルーフメモリ１００４の記憶領域のうち共有メモリとしては用いられる記憶領域以外の記憶領域は、データバス１００２を介してメディア・ドラブＳＡＭ２６０から入力したコンテンツデータをＡＶ圧縮・伸長用ＳＡＭ１６３に出力するまで一時的に記憶するために用いられる。

【０２５５】ＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵバス１０００を介してダウンロードメモリ１６７との間でデータ転送を行い、データバス１００２を介してメディア・ドラブＳＡＭ２６０との間でデータ転送を行う。

【０２５６】ホストＣＰＵバス１０００には、ダウンロードメモリ１６７の他に、ＳＡＭ１０５１、ＡＶ圧縮・伸長用ＳＡＭ１６３およびＤＭＡ(Direct Memory Access)１０１０が接続されている。ＤＭＡ１０１０は、ホストＣＰＵバス１０００を介したダウンロードメモリ１６７へのアクセスを、ホストＣＰＵ８１０１からの命令に応じて、統括的に制御する。また、ホストＣＰＵバス１０００は、１３９４シリアル・インターフェースのＬＩＮＫ層を用いてユーザホームネットワーク１０３内の他のＳＡＭ１０５２～１０５４と通信を行なう際に用いられる。

【０２５７】ドライブＣＰＵバス１００１には、ドライブＣＰＵ１００３、メディア・ドラブＳＡＭ２６０、ＲＦアンプ１００６、メディアＳＡＭインターフェイス１００７およびＤＭＡ１０１１が接続されている。ドライブＣＰＵ１００３は、例えば、ホストＣＰＵ８１０１からの命令を受けて、ディスク型の記録媒体１３０にアクセスを行う際の処理を統括的に制御する。この場合に、ホストＣＰＵ８１０１がマスタとなり、ドライブＣＰＵ１００３がスレーブとなる。ドライブＣＰＵ１００３は、ホストＣＰＵ８１０１から見てＩ／Ｏとして扱われる。ドライブＣＰＵ１００３は、例えばＲＡＭ型などの記録媒体１３０にアクセスを行う際のデータのエンコードおよびデコードを行う。ドライブＣＰＵ１００３は、ＲＡＭ型の記録媒体１３０がドライブにセットされると、ＲＡＭ型の記録媒体１３０がＳＡＭ１０５１による権利処理の対象となる（ＥＭＤシステム１００の対象となる）記録媒体であるか否かを判断し、当該記録媒体であると判断した場合に、そのことをホストＣＰＵ８１０１に通知すると共に、メディア・ドラブＳＡＭ２６０にメディアＳＡＭ１３３との間の相互認証などを行うことを指示する。

【０２５８】メディアＳＡＭインターフェイス１００７は、ドライブＣＰＵバス１００１を介した記録媒体１３０のメディアＳＡＭ１３３に対してのアクセスを行う際のインターフェイスとして機能する。ＤＭＡ１０１１は、例えば、ドライブＣＰＵ１００３からの命令に応じて、ドライブＣＰＵバス１００１およびデータバス１００２を介したショックプルーフメモリ１００４へのメモリアクセスを統括的に制御する。ＤＭＡ１０１１は、例えば、データバス１００２を介した、メディア・ドラブＳＡＭ２６０とショックプルーフメモリ１００４との間のデータ転送を制御する。

【０２５９】図６２に示す構成では、例えば、ＳＡＭ１０５１と記録媒体１３０のメディアＳＡＭ１３３との間で相互認証などの通信を場合には、ホストＣＰＵ８１０１の制御に基づいて、ホストＣＰＵバス１０００、ホストＣＰＵ８１０１、ドライブＣＰＵ１００３内のレジスタ、ドライブＣＰＵバス１００１およびメディアＳＡＭインターフェイス１００７を介して、ＳＡＭ１０５１とメディアＳＡＭ１３３との間でデータが転送される。また、記録媒体１３０にアクセスを行う場合には、メディア・ドラブＳＡＭ２６０とメディアＳＡＭ１３３との間で相互認証が行われる。また、前述したように、ダウンロードメモリ１６７およびショックプルーフメモリ１００４にアクセスを行うために、ＡＶ圧縮・伸長用ＳＡＭ１６３においてデータを圧縮または伸長する場合には、ＳＡＭ１０５１とＡＶ圧縮・伸長用ＳＡＭ１６３との間で相互認証が行われる。

【０２６０】本実施形態では、図６２において、ＳＡＭ１０５１およびＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵ８１０１からは、Ｉ／Ｏインターフェイスに接続されたデバイスとして扱われる。ＳＡＭ１０５１およびＡＶ圧縮・伸長用ＳＡＭ１６３とホストＣＰＵ８１０１との間の通信およびデータ転送は、メモリＩ／Ｏ＆アドレスデコーダ１０２０の制御に基づいて行われる。このとき、ホストＣＰＵ８１０１がマスタ(Master)になり、ＳＡＭ１０５１およびＡＶ圧縮・伸長用ＳＡＭ１６３がスレーブ(Slave)になる。ＳＡＭ１０５１およびＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵ８１０１からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をホストＣＰＵ８１０１に通知する。また、メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０は、ドライブＣＰＵ１００３からはＩ／Ｏインターフェイスに接続されたデバイスとして扱われる。メディアＳＡＭ１３３およびメディア・ドラブＳＡ

ＭＡＣ２６０とドライブＣＰＵ１００３との間の通信およびデータ転送は、メモリＩ／Ｏ＆アドレスデコーダ１０２１の制御に基づいて行われる。このとき、ドライブＣＰＵ１００３がマスタになり、メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０がスレーブになる。メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０は、ドライブＣＰＵ１００３からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をドライブＣＰＵ１００３に通知する。

【０２６１】また、ダウンロードメモリ１６７およびショックプルーフメモリ１００４に対してのコンテンツファイルＣＦおよびキーファイルＫＦに関するアクセス制御は、ＳＡＭ１０５１が統括的に行ってもよいし、あるいはコンテンツファイルＣＦのアクセス制御をホストＣＰＵ８１０１が行い、キーファイルＫＦのアクセス制御をＳＡＭ１０５１が行ってもよい。

【０２６２】ドライブＣＰＵ１００３によって記録媒体１３０から読み出されたコンテンツデータＣは、ＲＦアンプ１００６およびメディア・ドラブＳＡＭ２６０を経て、ショックプルーフメモリ１００４に格納され、その後、ＡＶ圧縮・伸長用ＳＡＭ１６３において伸長される。伸長されたコンテンツデータはＤ／Ａ変換器において、２でデジタルからアナログに変換され、当該変換によって得られたアナログ信号に応じた音響がスピーカから出力される。このとき、ショックプルーフメモリ１００４は、記録媒体１３０の隣接的に位置する記録領域から非連続的に読み出された複数のトラックのコンテンツデータＣを一時的に格納した後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に連続して出力してもよい。

【０２６３】以下、ユーザホームネットワーク１０３内の各種のＳＡＭが上述した機能を実現するために備える回路モジュールについて説明する。ユーザホームネットワーク１０３内のＳＡＭとしては、前述したように、購入形態の決定などの権利処理（利益分配）に係わる処理を行うＳＡＭ１０５（１０５１～１０５ｎ）と、記録媒体に設けられるメディアＳＡＭ１３３と、ＡＶ圧縮・伸長用ＳＡＭ１６３と、メディア・ドラブＳＡＭ２６０とがある。以下、これらのＳＡＭに設けられる回路モジュールをそれぞれ説明する。

【０２６４】＜権利処理用のＳＡＭの第１形態＞図６３は、権利処理用のＳＡＭ１０５ａの回路モジュールを説明するための図である。図６３に示すように、ＳＡＭ１０５ａは、ＣＰＵ１１００、ＤＭＡ１１０１、ＭＭＵ１１０２、Ｉ／Ｏモジュール１１０３、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０９、（真性）乱数発生器１１１０、リアルタイムクロックモジュール１１１１、外部バスＩ／Ｆ１１１２を有する耐タンパ性のハードウェア（Tamper Registant H/W）（水発明の回路モジュール）である。ここで、ＣＰＵ１１００が本発明の演算処理回路に対応し、ＤＭＡ１１０１が本発明の記憶回路制御回路に対応し、ＭＭＵ１１０２が本発明の記憶管理回路に対応し、Ｉ／Ｏモジュール１１０３が本発明のインターフェイスに対応し、マスクＲＯＭ１１０４、不揮発性メモリ１１０５およびf作業用ＲＡＭ１１０６が本発明の記憶回路に対応し、公開鍵暗号モジュール１１０７が本発明の公開鍵暗号回路に対応し、共通鍵暗号モジュール１１０８が本発明の共通鍵暗号回路に対応し、ハッシュ関数モジュール１１０９が本発明のハッシュ値生成回路に対応し、（真性）乱数発生器１１１０が本発明の乱数生成回路に対応し、リアルタイムクロックモジュール１１１１が本発明のリアルタイムクロックに対応し、外部バスＩ／Ｆ１１１２が本発明の外部バスインターフェイスに対応している。

【０２６５】図２３に示すＳＡＭ１０５１の機能モジュールと、図６３に示す回路モジュールとの関係を簡単に説明する。ＣＰＵ１１００は、例えば、マスクＲＯＭ１１０４および不揮発性メモリ１１０５に記憶されたプログラムを実行して、図２３に示す開金処理部１８７および利用監視部１８６の機能を実現する。ＤＭＡ１１０１は、ＣＰＵ１１００からの命令に応じて、図２２に示すダウンロードメモリ１６７および図２３に示す記憶部１９２に対してのアクセスを統括的に制御する。ＭＭＵ１１０２は、図２２に示すダウンロードメモリ１６７および図２３に示す記憶部１９２のアドレス空間を管理する。Ｉ／Ｏモジュール１１０３は、例えば、図２３に示すメディアＳＡＭ管理部１９７の一部の機能を実現する。マスクＲＯＭ１１０４には、ＳＡＭ１０５ａの初期化プログラムやインテグリティチェック（Integrity Check）プログラムなどの改変しないプログラムおよびデータが製造時に記憶され、図２３に示す記憶部１９２の…部の機能を実現する。不揮発性メモリ１１０５は、改変する可能性のある例えば暗号化プログラムや暗データなどを記憶し、図２３に示す記憶部１９２の一部の機能を実現する。作業用ＲＡＭ１１０６は、図２３に示す作業用メモリ２００に対応している。

【０２６６】公開鍵暗号モジュール１１０７は、図２３に示す署名処理部１８９の機能の一部を実現し、例えば、公開鍵暗号方式を用いた、メディアＳＡＭ１３３等と間の相互認証、ＳＡＭ１０５の署名データの作成、署名データ（ＥＭＤサービスセンタ１０２、コンテンツプロバイダ１０１、第２実施形態の場合にはサービスプロバイダ３１０の署名データ）の検証、データ量の少ないデータ（キーファイルＫＦなど）の転送を行う際の当該データの暗号化および復号、並びに、鍵共有を行う際に用いられる。公開鍵暗号モジュール１１０７は、回路モジュールとして実現してもよいし（H/W IP Solution）、不揮発性メモリ１１０５に記憶した公開鍵暗号プログラムをＣＰＵ１１００において実行して実現してもよい（S

/W IPSolution)。

【０２６７】共通鍵暗号モジュール１１０８は、図２３に示す署名処理部１８９、暗号化・復号部１７１，１７２，１７３の機能の一部を実現し、相互認証、相互認証によって得た共通鍵であるセッション鍵データKsesを用いたデータの暗号化および復号を行う際に用いられる。共通鍵暗号方式は、公開鍵暗号方式に比べて高速処理が可能であり、例えば、コンテンツデータ（コンテンツファイルＣＦ）などのデータ量が大きいデータを暗号化および復号する際に用いられる。共通鍵暗号モジュール１１０８は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１１０５に記憶した共通鍵暗号プログラムをＣＰＵ１１００において実行して実現してもよい(S/W IP Solution)。なお、相互認証は、公開鍵暗号モジュール１１０７による暗号・復号および共通鍵暗号モジュール１１０８による暗号・復号の何れか一方あるいは双方を採用する。

【０２６８】ハッシュ関数モジュール１１０９は、図２３に示す署名処理部１８９の機能の一部を実現し、署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール１１０９は、コンテンツプロバイダ１０１およびEMDサービスセンタ１０２などの署名データや、図３７に示すセキュアコンテナ１０４ｘのキーファイルKF1のハッシュ値Hx1を検証する際に用いられる。ハッシュ関数モジュール１１０９は、回路モジュールとして実現してもよいし(H/W IPSolution)、不揮発性メモリ１１０５に記憶したハッシュ回路モジュールをＣＰＵ１１００において実行して実現してもよい(S/W IP Solution)。

【０２６９】乱数発生器１１１０は、例えば、図２３に示す相互認証部１７０の機能の一部を実現する。リアルタイムクロックモジュール１１１１は、リアルタイムの時刻を発生する。当該時刻は、例えば、有効期限付きのライセンス鍵データKDを選択する場合や、利用制御データ１６６によって示される有効期限の要件を満たされているか否かを判断する際に用いられる。外部バスＩ／Ｆ１１１２は、図２３に示すコンテンツプロバイダ管理部１８０、ダウンロードメモリ管理部１８２およびEMDサービスセンタ管理部１８５の一部を機能を実現する。

【０２７０】図６４は、ＳＡＭ１０５ａ内のハードウェア構成を説明するための図である。図６４において、図６３に示したものと同じ回路モジュールには、図６３と同じ符号を付している。図６４に示すように、ＳＡＭ１０５ａ内では、ＳＡＭ・ＣＰＵバス１１２０を介してＣＰＵ１１００、マスクＲＯＭ１１０４および不揮発性メモリ１１０５が接続されている。内部バス１１２１には、ＤＭＡ１１０１が接続されている。内部バス１１２２には、I^2C・インターフェイス１１３０、メディアＳＡＭ・インターフェイス１１３１、ＭＳ(Memory Stick)・インターフェイス１１３２およびＩＣカード・インターフェイス１１３３が接続されている。メディアＳＡＭ・インターフェイス１１３１は記録媒体１３０のメディアＳＡＭ１３３との間でデータ転送を行う。ＭＳ・インターフェイス１１３２はメモリスティック１１４０との間でデータ転送を行う。ＩＣカード・インターフェイス１１３３はＩＣカード１１４１との間でデータ転送を行う。

【０２７１】外部バス１１２３には、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０９、乱数発生器１１１０、リアルタイムクロック生成モジュール１１１１および外部バスＩ／Ｆ１１１２が接続されている。

【０２７２】ＳＡＭ・ＣＰＵバス１１２０と内部バス１１２１とは、バス・インターフェイス１１１６を介して接続されている。内部バス１１２２と内部バス１１２１とは、バス・インターフェイス１１１７を介して接続されている。内部バス１１２１と外部バス１１２３とは、バス・インターフェイス１１１５を介して接続されている。

【０２７３】ＤＭＡ１１０１は、ＣＰＵ１１００からの命令に応じて、内部バス１１２１を介した、マスクＲＯＭ１１０４、不揮発性メモリ１１０５および作業用ＲＡＭ１１０６に対してのアクセスを統括的に制御する。ＭＭＵ１１１３は、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、図６２に示すダウンロードメモリ１６７のメモリ空間を管理する。アドレスデコーダ１１１４は、内部バス１１２１と外部バス１１２３との間でデータ転送を行う際に、アドレス変換を行う。また、書き込みロック制御回路１１３５は、ＣＰＵ１１００からのロック機能データに基づいて、フラッシュＲＯＭに対してのデータの書き込みおよび消去をブロック単位で管理する。

【０２７４】＜権利処理用のＳＡＭの第２形態＞図６５は、権利処理用のＳＡＭ１０５ｂの回路モジュールを説明するための図である。図６５では、ＳＡＭ１０５ａの構成要素と同じものには、図６４と同じ符号を付している。図６５に示すように、ＳＡＭ１０５ｂは、セキュアメモリ１０５ｂａ、ホストＣＰＵ８１０、耐タンパ性ソフトウェア１１３０、Ｉ／Ｏモジュール１１０３を用いて実現される。ＳＡＭ１０５ｂでは、ホストＣＰＵ８１０において、耐タンパ性ソフトウェア１１３０を実行することで、図６３に示すＣＰＵ１１００と同じ機能を実現する。耐タンパ性ソフトウェア１１３０は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。セキュアメモリ１０５ｂａには、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０

９、（真性）乱数発生器１１１０、リアルタイムクロックモジュール１１１１および外部バスＩ／Ｆ１１１２を有する耐タンパ性のハードウエアである。なお、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８およびハッシュ関数モジュール１１０９は、回路モジュールとして実現してもよいし(H/W IP Solution)、それぞれ本実施例メモリ１１０５に記憶した公開鍵暗号プログラム、共通鍵暗号プログラムおよびハッシュ関数プログラムをホストＣＰＵ８１０において実行して実現してもよい(S/W IP Solution)。

【０２７５】以下、前述したメディアＳＡＭ１３３として機能する各種のメディアＳＡＭの構成について説明する。

<メディアＳＡＭの第１形態>図６６は、メディアＳＡＭ１３３ａの回路モジュールを説明するための図である。図６６に示すように、メディアＳＡＭ１３３ａは、ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７、共通鍵暗号モジュール１２０８、ハッシュ関数モジュール１２０９、（真性）乱数発生器１２１０を有する耐タンパ性のハードウエア(Tamper Registant H/W)である。

【０２７６】ＣＰＵ１２００は、耐タンパ性のハードウエア内の各回路の制御を行う。

【０２７７】公開鍵暗号モジュール１２０７は、例えば、公開鍵暗号方式を用いた、例えば（１）：図６２に示すＳＡＭ１０５ｂおよびドライブＣＰＵ１００３等との間の相互認証、（２）メディアＳＡＭ１３３の署名データの作成、署名データ（EMDサービスセンタ１０２、コンテンツプロバイダ１０１、第２実施形態の場合にはサービスプロバイダ３１０の署名データ）の検証、（３）：転送されるデータ量の少ないメッセージの暗号化および復号、並びに、（４）：相互認証によって得たセッション鍵データK_{SES}の鍵共有を行う際に用いられる。公開鍵暗号モジュール１１０７は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶した公開鍵暗号プログラムをＣＰＵ１２００において実行して実現してもよい(S/W IPSolution)。

【０２７８】共通鍵暗号モジュール１２０８は、相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたキーファイルＫＦ，KF_1などのデータの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール１２０８は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶した共通鍵暗号プログラムをＣＰＵ１２００において実行して実現してもよい(S/W IP Solution)。なお、相互認証は、公開鍵暗号モジュール１２０７による暗号・復号および共通鍵暗号モジュール１２０８による暗号・復号の何れか一方あるいは双方を採用する。

【０２７９】ハッシュ関数モジュール１２０９は、データのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール１１０９は、図３７に示すセキュアコンテナ１０４ｘのキーファイルKF_1のハッシュ値H_{KI}を検証する際に用いられる。ハッシュ関数モジュール１２０９は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶したハッシュ回路モジュールをＣＰＵ１２００において実行して実現してもよい(S/W IP Solution)。

【０２８０】乱数発生器１２１０は、例えば、相互認証を行う際に用いられる。Ｉ／Ｏモジュール１２０３は、図６２に示すメディアＳＡＭ１／Ｆ１００７との間の通信を行う際に用いられる。

【０２８１】マスクＲＯＭ１２０４には、メディアＳＡＭ１３３ａの初期化プログラムやインテグリティチェック(Integrity Check) プログラムなどの改竄しないプログラムおよびデータが製造時に記憶される。不揮発性メモリ１２０５は、改竄する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

【０２８２】図６７は、メディアＳＡＭ１３３ａがＲＯＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３ａの出荷時にマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。図６７に示すように、ROM型の記録媒体の出荷時には、メディアＳＡＭ１３３ａには、メディアＳＡＭの識別子（ＩＤ）、記録用鍵データK_{STR}（メディア鍵データK_{MED}）、EMDサービスセンタ１０２の公開暗号データ$K_{ESC.P}$、ルート認証局９２の公開鍵データ$K_{R-CA.P}$、メディアＳＡＭ１３３ａの公開鍵証明書データCER_{USAM}、メディアＳＡＭ１３３ａの公開鍵データ$K_{USAM.S}$、メディアＳＡＭ１３３ａの秘密鍵データ$K_{USAM.P}$、リポケーションリスト、複製処理用データ、利益分配したいエンティティの識別子（ＩＤ）、メディアのタイプ（メディアの種別情報、ROMおよびＲＡＭの何れかを特定する情報）、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ、所定の検証値（ＭＡＣ値）などが記憶される。ここで、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ、並びに所定の検証値（ＭＡＣ値）は、EMDサービスセンタ１０２が管理するライセンス鍵データＫＤを用いて暗号化されている。

【０２８３】図６８は、メディアＳＡＭ１３３ａがＲＯＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３ａの出荷後のユーザ登録およびコンテンツデータの購入形態決定を行ったときにマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。図６８に示すように、メディアＳＡＭ１３

３ａには、ユーザ登録によって、新たに、ユーザＩＤ、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報、キーファイルＫＦｉなどのデータが書き込まれる。

【０２８４】図６９は、メディアＳＡＭ１３３ａがＲＡＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３ａの出荷時にマスクＲＯＭ１２０４およびオ揮発性メモリ１２０５に格納されているデータを示す図である。図６９に示すように、ＲＡＭ型の記録媒体の出荷時には、メディアＳＡＭ１３３ａには、メディアＳＡＭの識別子（ＩＤ）、記録用鍵データK_{STR}（メディア鍵データK_{MED}）、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ルート認証局９２の公開鍵データ$K_{R-CA,P}$、メディアＳＡＭ１３３ａの公開鍵証明書データCER_{MSAM}、メディアＳＡＭ１３３ａの公開鍵データ$K_{MSAM,P}$、メディアＳＡＭ１３３ａの秘密鍵データ$K_{MSAM,S}$、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子（ＩＤ）、メディアのタイプ（メディアの種別情報、ＲＯＭおよびＲＡＭの何れかを特定する情報）が記憶されており、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，ＫＦｉ、所定の検証値（ＭＡＣ値）などは記憶されていない。

【０２８５】図７０は、メディアＳＡＭ１３３ａがＲＡＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３ａの出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。図６６に示すように、メディアＳＡＭ１３３ａには、ユーザ登録によって、新たに、ユーザＩＤ、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報などのデータに加えて、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，ＫＦｉ，並びに所定の検証値（ＭＡＣ値）が書き込まれる。キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，ＫＦｉ，並びに所定の検証値（ＭＡＣ値）は、記録用鍵データK_{STR}によって暗号化されている。

【０２８６】＜メディアＳＡＭの第２形態＞図７１は、メディアＳＡＭ１３３ｂの回路モジュールを説明するための図である。図７１に示すように、メディアＳＡＭ１３３ｂは、ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７、ハッシュ関数モジュール１２０９、（真性）乱数発生器１２１０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアＳＡＭ１３３ｂは、図６６に示すメディアＳＡＭ１３３ａから、共通鍵暗号モジュール１２０８を除いた構成をしている。

【０２８７】メディアＳＡＭ１３３ｂの公開鍵暗号モジュール１２０７は、（１）：図６２に示すＳＡＭ１０５１およびドライブＣＰＵ１００３等と間の相互認証、（２）メディアＳＡＭ１３３の署名データの作成、署名データ（ＥＭＤサービスセンタ１０２、コンテンツプロバイダ１０１、第２実施形態の場合にはサービスプロバイダ３１０の署名データ）の検証、（３）：転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアＳＡＭ１３３ａの公開鍵暗号モジュール１２０７とは異なり、（４）：相互認証によって得たセッション鍵データK_{SES}の鍵共有は行わない。鍵の共有を行わないのは、共通鍵暗号モジュール１２０８を有していないためである。また、メディアＳＡＭ１３３ｂの公開鍵暗号モジュール１２０７は、公開鍵暗号方式を用いて、さらにキーファイルＫＦ，ＫＦｉなどのデータの暗号化および復号を行う。

【０２８８】＜メディアＳＡＭの第３形態＞図７２は、メディアＳＡＭ１３３ｃの回路モジュールを説明するための図である。図７２に示すように、メディアＳＡＭ１３３ｃは、ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７、（真性）乱数発生器１２１０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアＳＡＭ１３３ｃは、図６６に示すメディアＳＡＭ１３３ａから、共通鍵暗号モジュール１２０８およびハッシュ関数モジュール１２０９を除いた構成をしている。メディアＳＡＭ１３３ｃの公開鍵暗号モジュール１２０７は、（１）：図６２に示すＳＡＭ１０５１およびドライブＣＰＵ１００３等と間の相互認証、（２）メディアＳＡＭ１３３の署名データの作成、（３）：転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアＳＡＭ１３３ａの公開鍵暗号モジュール１２０７とは異なり、署名データの検証および（４）：相互認証によって得たセッション鍵データK_{SES}の鍵共有は行わない。署名データの検証を行わないのは、ハッシュ関数モジュール１２０９を有していないためである。また、メディアＳＡＭ１３３ｃの公開鍵暗号モジュール１２０７は、公開鍵暗号方式を用いて、キーファイルＫＦ，ＫＦｉなどのデータの暗号化および復号を行う。この場合に、メディアＳＡＭ１３３ｃは、署名データの検証を行わないため、ＳＡＭ１０５から公開鍵データ$K_{SP,P}$，$K_{ESC,P}$（第２実施形態の場合には、さらにサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$）を受ける。

【０２８９】＜メディアＳＡＭの第４形態＞図７３は、

メディアＳＡＭ１３３ｄの回路モジュールを説明するための図である。図７３に示すように、メディアＳＡＭ１３３ｄは、ＣＰＵ１２００、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７、（真性）乱数発生器１２１０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアＳＡＭ１３３ｃは、図６６に示すメディアＳＡＭ１３３ａから、ＤＭＡ１２０１、共通鍵暗号モジュール１２０８およびハッシュ関数モジュール１２０９を除いた構成をしている。メディアＳＡＭ１３３ｄの公開鍵暗号モジュール１２０７は、基本的に、前述したメディアＳＡＭ１３３ｃの公開鍵暗号モジュール１２０７と同じ機能を有している。メディアＳＡＭ１３３ｄは、ＤＭＡ１２０１を有していないため、マスクＲＯＭ１２０４、不揮発性メモリ１２０５および作業用ＲＡＭ１２０６に対してのアクセス制御はＣＰＵ１２００によって行われる。

【０２９０】＜メディアＳＡＭの第５形態＞図７４は、メディアＳＡＭ１３３ｅの回路モジュールを説明するための図である。図７４に示すように、メディアＳＡＭ１３３ｅは、セキュアメモリ１３３ｅａ、ホストＣＰＵ８１０および耐タンパ性ソフトウェア１１３０を用いて実現される。セキュアメモリ１３３ｅａは、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７および（真性）乱数発生器１２１０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。セキュアメモリ１３３ｅａ内の各モジュールは、同一符号のメディアＳＡＭ１３３ｄのモジュールと同じである。

【０２９１】すなわち、セキュアメモリ１３３ｅａは、図７３に示すメディアＳＡＭ１３３Ｄから、ＣＰＵ１２００を除いた構成をしている。ＳＡＭ１０５ｅでは、ホストＣＰＵ８１０において、耐タンパ性ソフトウェア１２５０を実行することで、図７３に示すＣＰＵ１２００と同じ機能を実現する。耐タンパ性ソフトウェア１２５０は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

【０２９２】＜メディアＳＡＭの第６形態＞図７５は、メディアＳＡＭ１３３ｆの回路モジュールを説明するための図である。図７５に示すように、メディアＳＡＭ１３３ｆは、ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６および公開鍵暗号モジュール１２０７を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。すなわち、メディアＳＡＭ１３３ｆは、図７２に示すメディアＳＡＭ１３３Ｃから、乱数生成器１２１０を除いた構成をしている。メディアＳＡＭ１３３ｆの公開鍵暗号モジュール１２０７は、（２）メディアＳＡＭ１３３の署名データの作成、（３）：転送されるデータ量の少ないメッセージの暗号化および復号を行うが、前述したメディアＳＡＭ１３３ａの公開鍵暗号モジュール１２０７とは異なり、署名データの検証、相互認証および（４）：相互認証によって得たセッション鍵データＫｓｅｓ の鍵共有は行わない。この場合に、メディア・ドラブＳＡＭ２６０からメディアＳＡＭ１３３ｆの認証は行われるが、メディアＳＡＭ１３３ｆが乱数生成器１２１０を有していないため、メディアＳＡＭ１３３ｆからメディア・ドラブＳＡＭ２６０の認証は行わない。

【０２９３】＜メディアＳＡＭの第７形態＞図７６は、メディアＳＡＭ１３３ｇの回路モジュールを説明するための図である。図７６に示すように、メディアＳＡＭ１３３ｇは、セキュアメモリ１３３ｇａ、ホストＣＰＵ８１０および耐タンパ性ソフトウェア１２６０を用いて実現される。図７６に示すように、セキュアメモリ１３３ｇａは、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６および公開鍵暗号モジュール１２０７を有する耐タンパ性のハードウェア(TamperRegistant H/W)である。すなわち、メディアＳＡＭ１３３ｇａは、図７５に示すメディアＳＡＭ１３３ｆから、ＣＰＵ１２００およびＤＭＡ１２０１を除いた構成をしている。メディアＳＡＭ１３３ｇの公開鍵暗号モジュール１２０７の機能は、基本的に前述したメディアＳＡＭ１３３ｆの公開鍵暗号モジュール１２０７と同じである。ＳＡＭ１０５ｇでは、ホストＣＰＵ８１０において、耐タンパ性ソフトウェア１２６０を実行することで、図７５に示すＣＰＵ１２００と同じ機能を実現する。耐タンパ性ソフトウェア１２６０は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

【０２９４】＜ＡＶ圧縮・伸長ＳＡＭ１６３＞ＡＶ圧縮・伸長ＳＡＭ１６３は、例えば、図２２を用いて既明した機能を実現する。図７７は、ＡＶ圧縮・伸長ＳＡＭ１６３の回路モジュールを説明するための図である。図７７に示すように、ＡＶ圧縮・伸長ＳＡＭ１６３は、ＣＰＵ／ＤＳＰ１３００、ＤＭＡ１３０１、マスクＲＯＭ１３０４、不揮発性メモリ１３０５、作業用ＲＡＭ１３０６、共通鍵暗号モジュール１３０８、（真性）乱数発生器１３１０、圧縮・伸長モジュール１３２０、電子透かし情報付加・検出モジュール１３２１および情報半開示制御モジュール１３２２を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【０２９５】ＣＰＵ／ＤＳＰ１３００は、例えば、図６２に示すＳＡＭ１０５ｉからの命令に応じて、マスクＲＯＭ１３０４および不揮発性メモリ１３０５に記憶されたプログラムを実行し、ＡＶ圧縮・伸長用ＳＡＭ１６３

内の各回路モジュールを統括的に制御する。ＤＭＡ１３０１は、ＣＰＵ／ＤＳＰ１３００からの命令に応じて、マスクＲＯＭ１３０４、不揮発性メモリ１３０５、作業用ＲＡＭ１３０６に対してのアクセスを統括的に制御する。マスクＲＯＭ１３０４には、ＡＶ圧縮・伸長用ＳＡＭ１６３の初期化プログラムやインテグリティチェック（Integrity Check）プログラムなどの改変しないプログラムや、ＡＶ圧縮・伸長用ＳＡＭ１６３の識別子であるＡＶＳＡＭ__ＩＤなどの改変しないデータが製造時に記憶される。不揮発性メモリ１３０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用ＲＡＭ１３０６は、ＳＡＭ１０５１から入力したキーファイルＫＦなどを記憶する。

【０２９６】共通鍵暗号モジュール１３０８は、ＳＡＭ１０５１との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたコンテンツデータなどの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール１３０８は、回路モジュールとして実現してもよいし（Ｈ／Ｗ ＩＰ Solution）、不揮発性メモリ１３０５に記憶した共通鍵暗号プログラムをＣＰＵ／ＤＳＰ１３００において実行して実現してもよい（S/W IP Solution）。また、共通鍵暗号モジュール１３０８は、権利処理用のＳＡＭから入力したコンテンツ鍵データＫｃを用いて、コンテンツデータの復号を行う。乱数発生器１１１０は、例えば、ＳＡＭ１０５１との間の相互認証処理を行う際に用いられる。

【０２９７】圧縮・伸長モジュール１３２０は、例えば、図２２に示す伸長部２２３の機能を実現し、図６２に示すダウンロードメモリ１６７およびショックプルーフメモリ１００４から入力したコンテンツデータの伸長処理と、Ａ／Ｄ変換器から入力したコンテンツデータの圧縮処理とを行う。

【０２９８】電子透かし情報添付・検出モジュール１３２１は、図２２に示す電子透かし情報処理部２２４の機能を実現し、例えば、圧縮・伸長モジュール１３２０の処理対象となるコンテンツデータに対して所定の電子透かし情報を埋め込むと共に、当該コンテンツデータに埋め込まれた電子透かし情報を検出し、圧縮・伸長モジュール１３２０による処理の適否を判断する。

【０２９９】情報半開示制御モジュール１３２２は、図２２に示す半開示処理部２２５の機能を実現し、必要に応じて、コンテンツデータを半開示状態で再生する。

【０３００】なお、ＡＶ圧縮伸長ＳＡＭ１６３として、例えば、コンテンツファイルＣＦに格納された図３に示すＡ／Ｖ伸長用ソフトウェアＳｏｆｔおよび電子透かし情報モジュールＷＭを用いて処理を行う場合には、図７８に示すように、図７７に示す構成から圧縮・伸長モジュール１３２０および電子透かし情報添付・検出モジュール１３２１を除いた構成にすることができる。このようにすることで、ＡＶ圧縮伸長用ＳＡＭ１６３において、コンテンツプロバイダ１０１の要求に応じた任意の伸長処理および電子透かし処理を行うことができる。

【０３０１】<メディア・ドラブＳＡＭ２６０の第１形態>図７９は、メディア・ドラブＳＡＭ２６０ａの回路モジュールを説明するための図である。図７９に示すように、メディア・ドラブＳＡＭ２６０ａは、ＣＰＵ１４００、ＤＭＡ１４０１、マスクＲＯＭ１４０４、不揮発性メモリ１４０５、作業用ＲＡＭ１４０６、共通鍵暗号モジュール１４０８、ハッシュ関数モジュール１４０９、（真性）乱数発生器１４１０、エンコーダ・デコーダモジュール１４２０、記録用鍵データ生成モジュール１４３０およびメディア・ユニークＩＤ生成モジュール１４４０を有する耐タンパ性のハードウェア（Tamper Registant H/W）である。

【０３０２】ＣＰＵ１４００は、例えば、図６２に示すドライブＣＰＵ１００３からの命令に応じて、マスクＲＯＭ１４０４および不揮発性メモリ１４０５に記憶されたプログラムを実行し、メディア・ドラブＳＡＭ２６０ａ内の各回路モジュールを統括的に制御する。ＤＭＡ１４０１は、ＣＰＵ１４００からの命令に応じて、マスクＲＯＭ１４０４、不揮発性メモリ１４０５、作業用ＲＡＭ１４０６に対してのアクセスを統括的に制御する。マスクＲＯＭ１４０４には、メディア・ドラブＳＡＭ２６０ａの初期化プログラムやインテグリティチェック（Integrity Check）プログラムなどの改変しないプログラムや、メディア・ドラブＳＡＭ２６０ａの識別子であるＭＤＳＡＭ__ＩＤなどの改変しないデータが製造時に記憶される。不揮発性メモリ１４０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用ＲＡＭ１４０６は、種々の処理を行う際の作業用メモリとして用いられる。

【０３０３】共通鍵暗号モジュール１４０８は、メディアＳＡＭ１３３およびＡＶ圧縮・伸長用ＳＡＭ１６３との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたコンテンツファイルＣＦおよびキーファイルＫＦなどの暗号化および復号、並びに記録用鍵データK_{STR}を用いたコンテンツ鍵データＫｃの暗号化などを行う際に用いられる。また、共通鍵暗号モジュール１４０８は、共通鍵データと署名の対象となるデータのハッシュ値を用いて、署名データの検証および作成を行う。共通鍵暗号モジュール１４０８は、回路モジュールとして実現してもよいし（Ｈ／Ｗ ＩＰSolution）、不揮発性メモリ１４０５に記憶した共通鍵暗号プログラムをＣＰＵ１４００において実行して実現してもよい（S/W IP Solution）。なお、記録用鍵データK_{STR}を用いたコンテンツ鍵データＫｃの暗号化は、メディア・ドラブＳＡＭ２６０の共通鍵暗号モジュール１４０８およびメディアＳＡＭ１３３の何れで行ってもよい。ハッシュ関数モジュール１４０９は、署名データの検証、並びに署名データを作成する対象となるデータのハッシュ

値を生成する際に用いられる。乱数発生器１４１０は、例えば、メディアＳＡＭ１３３との間の相互認証処理を行う際に用いられる。

【０３０４】エンコーダ・デコーダモジュール１４２０は、記録媒体１３０のＲＯＭ領域あるいはＲＡＭ領域に対して、コンテンツデータのアクセスを行う際に、当該コンテンツデータのエンコード処理、デコード処理、ＥＣＣ(Error Correction Code) 処理、変調処理、復調処理、セクタライズ処理およびデセクタライズ処理などを行う。

【０３０５】記録用鍵データ生成モジュール１４３０は、メディア・ユニークＩＤ生成モジュール１４４０が生成したメディア・ユニークＩＤを用いて、各メディアにユニークな記録用鍵データK_{STR} を生成する。

【０３０６】メディア・ユニークＩＤ生成モジュール１４４０は、メディア・ドラブＳＡＭ２６０で生成したドライブＩＤと、メディアＳＡＭ１３３のメディアＳＡＭ＿ＩＤとから、各記録媒体（メディア）にユニークなメディア・ユニークＩＤを生成する。

【０３０７】また、図８０に示すように、図７９に示すメディア・ドライブＳＡＭ２６０ａにおいて共通鍵暗号モジュール１４０８の代わりに公開鍵暗号モジュール１４０７を用いた構成のメディア・ドライブＳＡＭ２６０ｃ用いてもよい。

【０３０８】＜メディア・ドラブＳＡＭ２６０の第２形態＞図８１は、メディア・ドラブＳＡＭ２６０ｂを説明するための図である。図８１では、メディア・ドラブＳＡＭ２６０ａの構成装置と同じものには、図７８と同じ符号を付している。図８１に示すように、メディア・ドラブＳＡＭ２６０ｂは、セキュアメモリ２６０ｂａ、図６２に示すドライブＣＰＵ１００３、耐タンパ性ソフトウェア１４５０を用いて実現される。メディア・ドラブＳＡＭ２６０ｂでは、ドライブＣＰＵ１００３において、耐タンパ性ソフトウェア１４５０を実行することで、図８０に示すＣＰＵ１４００と同じ機能を実現する。耐タンパ性ソフトウェア１４５０は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。セキュアメモリ２６０ｂａは、マスクＲＯＭ１４０４、不揮発性メモリ１４０５、作業用ＲＡＭ１４０６、共通鍵暗号モジュール１４０８、ハッシュ関数モジュール１４０９、（真性）乱数発生器１４１０、エンコーダ・デコーダモジュール１４２０、記録用鍵データ生成モジュール１４３０およびメディア・ユニークＩＤ生成モジュール１４４０を有する耐タンパ性のハードウェア(Tamper Registant H/W) である。

【０３０９】また、図８２示すように、図８１に示すメディア・ドライブＳＡＭ２６０ｂおいて共通鍵暗号モジュール１４０８の代わりに公開鍵暗号モジュール１４０７を用いた構成のメディア・ドライブＳＡＭ２６０ｄ用

いてもよい。

【０３１０】以下、図１に示すＥＭＤシステム１００の全体動作について説明する。図８３は、コンテンツプロバイダ１０１の全体動作のフローチャートである。

ステップＳ１：ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１が所定の登録処理を経た後に、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をコンテンツプロバイダ１０１に送信する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５１～１０５４が所定の登録処理を経た後に、ＳＡＭ１０５１～１０５４の公開鍵データ$K_{SAM1,P}$～$K_{SAM4,P}$の公開鍵証明書CER_{CP1}～CER_{CP4}をＳＡＭ１０５１～１０５４に送信する。また、ＥＭＤサービスセンタ１０２は、相互認証を行った後に、各々有効期限が１カ月の３カ月分のライセンス鍵データKD_1～KD_3をユーザホームネットワーク１０３のＳＡＭ１０５１～１０５４に送信する。このように、ＥＭＤシステム１００では、ライセンス鍵データKD_1～KD_3を予めＳＡＭ１０５１～１０５４に配給しているため、ＳＡＭ１０５１～１０５４とＥＭＤサービスセンタ１０２との間がオフラインの状態でも、ＳＡＭ１０５１～１０５４においてコンテンツプロバイダ１０１から配給されたセキュアコンテナ１０４を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ１０８に記述され、利用履歴データ１０８は、ＳＡＭ１０５１～１０５４とＥＭＤサービスセンタ１０２とが接続されたときに、ＥＭＤサービスセンタ１０２に自動的に送信されるため、ＥＭＤサービスセンタ１０２における決済処理を確実に行うことができる。なお、ＥＭＤサービスセンタ１０２が、所定の期間内に、利用履歴データ１０８を回収できないＳＡＭについては、リボケーションリストで無効の対象とする。なお、利用側状態データ１６６は、原則として、リアルタイムで、ＳＡＭ１０５１～１０５４からＥＭＤサービスセンタ１０２に送信される。

【０３１１】ステップＳ２：コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で相互認証を行った後に、権利書データ１０６およびコンテンツ鍵データK_CをＥＭＤサービスセンタ１０２に安鍵して複改化する。また、ＥＭＤサービスセンタ１０２は、６カ月分のキーファイルK_Fを作成し、これをコンテンツプロバイダ１０１に送信する。

【０３１２】ステップＳ３：コンテンツプロバイダ１０１は、図３（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{4,CP}$と、キーファイルK_Fおよびその署名データ$SIG_{7,CP}$とを作成し、これらと図３（Ｃ）に示す公開鍵証明書データCER_{ESC}およびその署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク１０３のＳＡＭ１０５１～１０５４に配給する。オンラインの場合には、コンテ

ンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ１０４がコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。また、オフラインの場合には、ＲＯＭ型あるいはＲＡＭ型の記録媒体に記録された状態で、セキュアコンテナ１０４が、コンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。

【０３１３】ステップＳ４：ユーザホームネットワーク１０３のＳＡＭ１０５１～ＳＡＭ１０５ｎは、コンテンツプロバイダ１０１から配給を受けたセキュアコンテナ１０４内の署名データ$SIG_{S,CP}$，$SIG_{T,CP}$，$SIG_{K1,ESG}$を検証して、コンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認した後に、対応する期間のライセンス鍵データＫＤ１～ＫＤｓを用いてキーファイルＫＦを復号する。

【０３１４】ステップＳ５：ＳＡＭ１０５１～ＳＡＭ１０５ｎにおいて、ユーザによる図２２に示す購入・利用形態決定操作部１６５の操作に応じた操作信号Ｓ１６５に基づいて、購入・利用形態を決定する。このとき、図３０に示す利用監視部１８６において、セキュアコンテナ１０４に格納された権利書データ１０６に基づいて、ユーザによるコンテンツファイルＣＦの購入・利用形態が管理される。

【０３１５】ステップＳ６：ＳＡＭ１０５１～ＳＡＭ１０５ｎの図３０に示す課金処理部１８７において、操作信号Ｓ１６５に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ１０８および利用制御状態データ１６６が生成し、これらをＥＭＤサービスセンタ１０２に送信する。

【０３１６】ステップＳ７：ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を作成する。ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データSIG_{SS}を、図１に示すペイメントゲートウェイ９０を介して、決済機関９１に送信する。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０３１７】ステップＳ８：　決済機関９１において、署名データSIG_{SS}の検証を行った後に、決済請求権データ１５２に基づいて、ユーザが支払った金額が、コンテンツプロバイダ１０１の所有者に分配される。

【０３１８】以上説明したように、ＥＭＤシステム１００では、図３に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配給し、セキュアコンテナ１０４内のキーファイルＫＦについての処理をＳＡＭ１０５１～１０５ｎ内で行う。また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データKD_1～KD_3を用いて暗号化されており、配信鍵データKD_1～KD_3を保持しているＳＡＭ１０５１～１０５ｎ内でのみ復号される。そして、ＳＡＭ１０５１～１０５ｎでは、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。従って、ＥＭＤシステム１００によれば、ユーザホームネットワーク１０３におけるコンテンツデータＣの購入および利用を、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。

【０３１９】また、ＥＭＤシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ１０４を用いて行うことで、ＳＡＭ１０５１～１０５ｎにおけるコンテンツデータＣの権利処理を双方の場合において共通化できる。

【０３２０】また、ＥＭＤシステム１００では、ユーザホームネットワーク１０３内のネットワーク機器１６０１およびＡＶ機器１６０２～１６０ｎにおいてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【０３２１】図８４は、第１実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。図８４に示すように、マルチプロセッサシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を配送するプロトコルとして例えばＴＣＰ／ＩＰおよびＸＭＬ／ＳＭＩＬが用いられる。また、ユーザホームネットワーク１０３のＳＡＭ相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク１０３と１０３ａとの間でセキュアコンテナを転送するプロトコルとして例えば１３９４シリアルバス・インタフェース上に構築されたＸＭＬ／ＳＭＩＬが用いられる。また、この場合に、ＲＯＭ型やＲＡＭ型の記録媒体にセキュアコンテナを記録してＳＡＭ相互間で配送してもよい。

【０３２２】第２実施形態

上述した実施形態では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ１０５１～１０５ｎにコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのＳＡＭに配給する場合について説明する。

【０３２３】図８５は、本実施形態のＥＭＤシステム３

101

０００の構成図である。図８５に示すように、ＥＭＤシステム３００は、コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ユーザホームネットワーク３０３、サービスプロバイダ３１０、ペイメントゲートウェイ１９０および決済機関９１を有する。コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ＳＡＭ３０５１～３０５４およびサービスプロバイダ３１０は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。コンテンツプロバイダ３０１は、サービスプロバイダ３１０に対してコンテンツデータを供給する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ１０１およびＳＡＭ５０５１～５０５４に加えて、サービスプロバイダ３１０に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第１実施形態のＥＭＤサービスセンタ１０２と同じである。また、ユーザホームネットワーク３０３は、ネットワーク機器３６０１およびＡＶ機器３６０$_2$～３６０$_4$を有している。ネットワーク機器３６０１はＳＡＭ３０５１およびＣＡモジュール３１１を内蔵しており、ＡＶ機器３６０$_2$～３６０$_4$はそれぞれＳＡＭ３０５$_2$～３０５$_4$を内蔵している。ここで、ＳＡＭ３０５１～３０５４は、サービスプロバイダ３１０からセキュアコンテナ３０４の配給を受ける点と、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０についての署名データの検証処理およびＳＰ用購入履歴データ（データ配給装置用購入履歴データ）３０９の作成を行なう点とを除いて、前述した第１実施形態のＳＡＭ１０５１～１０５４と同じである。

【０３２４】先ず、ＥＭＤシステム３００の概要について説明する。ＥＭＤシステム３００では、コンテンツプロバイダ３０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す前述した第１実施形態と同様の権利書（UGP:Usage Control Policy）データ１０６およびコンテンツ鍵データＫｃを、高い信頼性のある権威機関であるＥＭＤサービスセンタ３０２に送信する。権利書データ１０６およびコンテンツ鍵データＫｃは、ＥＭＤサービスセンタ３０２に登録されて権威化（認証）される。

【０３２５】また、コンテンツプロバイダ３０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成する。また、コンテンツプロバイダ３０１は、ＥＭＤサービスセンタ３０２から、各コンテンツファイルＣＦについて、それぞれ６か月分のキーファイル・ＫＦを受信する。当該キーファイルＫＦ内には、当該キーファイルＫＦの改竄の有無、当該キーファイルＫＦの作成者および送信者の正当性を検証するための署名データが格納されている。そして、コンテンツプロバイダ３０１は、コンテンツファイルＣＦ、

102

キーファイルＫＦおよび自らの署名データとを格納した図３に示すセキュアコンテナ１０４を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ３１０に供給する。また、セキュアコンテナ１０４に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【０３２６】サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４を受け取ると、署名データの検証を行なって、セキュアコンテナ１０４の作成者および送信者の確認する。次に、サービスプロバイダ３１０は、例えばオフラインで通知されたコンテンツプロバイダ３０１が希望するコンテンツに対しての価格（ＳＲＰ）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（ＰＴ：本発明の価格データ）３１２を作成する。そして、サービスプロバイダ３１０は、セキュアコンテナ１０４から取り出したコンテンツファイルＣＦおよびキーファイルＫＦと、プライスタグデータ３１２と、これらに対しての自らの秘密鍵データ$K_{SP,S}$による署名データとを格納したセキュアコンテナ３０４を作成する。このとき、キーファイルＫＦは、ライセンス鍵データＫＤ１～ＫＤ$_6$によって暗号化されており、サービスプロバイダ３１０は当該ライセンス鍵データＫＤ１～ＫＤ$_6$を保持していないため、サービスプロバイダ３１０はキーファイルＫＦの中身を見たり、書き換えたりすることはできない。また、ＥＭＤサービスセンタ３０２は、プライスタグデータ３１２を登録して権威化する。

【０３２７】サービスプロバイダ３１０は、オンラインおよび／またはオフラインでセキュアコンテナ３０４をユーザホームネットワーク３０３に記録する。このとき、オフラインの場合には、セキュアコンテナ３０４はＲＯＭ型の記録媒体などに記録されてＳＡＭ３０５１～３０５４にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ３１０とＣＡモジュール３１１との間で相互認証を行い、セキュアコンテナ３０４をサービスプロバイダ３１０においてセッション鍵データK_{SES}を用いた暗号化して送信し、ＣＡモジュール３１１において受信したセキュアコンテナ３０４をセッション鍵データK_{SES}を用いて復号した後に、ＳＡＭ３０５１～３０５４に転送する。この場合に、コンテンツプロバイダ３０１からユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する通信プロトコルとして、デジタル放送であればＭＨＥＧ（Multimedia and Hypermedia information coding Experts Group）プロトコルが用いられ、インターネットであればＸＭＬ／ＳＭＬ／ＨＴＭＬ（Hyper TextMarkup Language）が用いられ、これらの通信プロトコル内に、セキュアコンテナ３

０４が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。従って、通信プロコトルとセキュアコンテナ３０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ３０４のフォーマットを柔軟に設定できる。

【０３２８】次に、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４内に格納された署名データを検証して、セキュアコンテナ３０４に格納されたコンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認する。そして、ＳＡＭ３０５$_1$～３０５$_4$において、当該正当性が確認されると、ＥＭＤサービスセンタ３０２から配給された対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_3$を用いてキーファイルＫＦを復号する。ＳＡＭ３０５$_1$～３０５$_4$に供給されたセキュアコンテナ３０４は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ３０５$_1$～３０５$_4$は、上述したセキュアコンテナ３０４の購入・利用の履歴を利用履歴（Usage Log）データ３０８として記録する。利用履歴データ（履歴データまたは管理簿履用履歴データ）３０８は、例えば、ＥＭＤサービスセンタ３０２からの要求に応じて、ユーザホームネットワーク３０３からＥＭＤサービスセンタ３０２に送信される。また、ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御データ（ＵＣＳ:Usage control state Data）１６６をＥＭＤサービスセンタ３０２に送信する。

【０３２９】ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１およびサービスプロバイダ３１０に分配される。

【０３３０】本実施形態では、ＥＭＤサービスセンタ３０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、ＥＭＤサービスセンタ３０２は、中立の立場にある最高の権威機関であるルート認証局９２に対してのセカンド認証局（Second Certificate Authority）としての役割を果たし、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ３０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ

３０１の権利書データ１０６、コンテンツ鍵データＫｃおよびサービスプロバイダ３１０のプライスタグデータ３１２を登録して権威化することも、ＥＭＤサービスセンタ３０２の認証機能によるものである。また、ＥＭＤサービスセンタ３０２は、例えば、ライセンス鍵データＫＤ$_1$～ＫＤ$_3$などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１が登録した権利書データ１０６とＳＡＭ３０５$_1$～ＳＡＭ３０５$_4$から入力した利用履歴データ３０８とサービスプロバイダ３１０が登録したプライスタグデータ３１２とに基づいて、ユーザホームネットワーク３０３のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ３０１およびサービスプロバイダ３１０に分配して支払う権利処理（利益分配）機能を有する。

【０３３１】以下、コンテンツプロバイダ３０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ３０１〕コンテンツプロバイダ３０１は、図３に示すセキュアコンテナ１０４をオンラインあるいはオフラインでサービスプロバイダ３１０に提供する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。すなわち、コンテンツプロバイダ３０１は、前述した図１７～図１９に示す手順でセキュアコンテナ１０４を作成し、セキュアコンテナ１０４を、コンテンツプロバイダ用商品配送プロトコルに挿入する。そして、サービスプロバイダ３１０が、ダウンロードを行って、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ１０４を取り出す。

【０３３２】〔サービスプロバイダ３１０〕サービスプロバイダ３１０は、コンテンツプロバイダ３０１から提供を受けたセキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦと、自らが生成したプライスタグデータ３１２とを格納したセキュアコンテナ３０４を作成し、ユーザホームネットワーク３０３のネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$にセキュアコンテナ３０４をオンラインおよび／またはオフラインで配給する。サービスプロバイダ３１０によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、ＣＭ（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【０３３３】サービスプロバイダ３１０は、コンテンツ

プロバイダ３０１からセキュアコンテナ１０４の提供を受けると、以下に示す処理を行ってセキュアコンテナ３０４を作成する。以下、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４からセキュアコンテナ３０４を作成し、これをユーザホームネットワーク３０３に配給する際のサービスプロバイダ３１０内での処理の流れを図８６を参照しながら説明する。図８６は、コンテンツプロバイダ３０１からユーザホームネットワーク３０３にセキュアコンテナ３０４を配給する処理を説明するためのフローチャートである。

＜ステップＳ８６－１＞サービスプロバイダ３１０は、オンラインおよび／またはオフラインで、コンテンツプロバイダ３０１から図３に示すセキュアコンテナ１０４の供給を受け、これを格納する。このとき、オンラインの場合には、コンテンツプロバイダ３０１とサービスプロバイダ３１０との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４を復号する。

＜ステップＳ８６－２＞サービスプロバイダ３１０は、セキュアコンテナ１０４の図３（Ｃ）に示す署名データ$SIG_{1,ESG}$を、ＥＭＤサービスセンタ３０２の公開鍵データ$KESG,P$を用いて検証し、その正当性が認められた後に、図３（Ｃ）に示す公開鍵証明書データ$CERGP$から公開鍵データKGP,Pを取り出す。次に、サービスプロバイダ３１０は、当該取り出した公開鍵データKGP,Pを用いて、セキュアコンテナ１０４の図３（Ａ），

（Ｂ）に示す署名データ$SIG_{8,GP}$，$SIG_{7,GP}$の検証、すなわちコンテンツファイルＣＦの作成者および送信者と、キーファイルＫＦの送信者との正当性の検証を行う。また、サービスプロバイダ３１０は、公開鍵データ$KESG,P$を用いて、図３（Ｂ）に示すキーファイルＫＦに格納された署名データ$SIG_{K1,ESG}$の検証、すなわちキーファイルＫＦの作成者の正当性の検証を行う。このとき、署名データ$SIG_{K1,ESG}$の検証は、キーファイルＫＦがＥＭＤサービスセンタ３０２に登録されているか否かの検証も施行いる。

【０３３４】＜ステップＳ８６－３＞サービスプロバイダ３１０は、例えばコンテンツプロバイダ３０１からオフラインで通知されたコンテンツプロバイダ３０１が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ３１２を作成する。また、サービスプロバイダ３１０は、コンテンツファイルＣＦ、キーファイルＫＦおよびプライスタグデータ３１２のハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データKSP,Pを用いて、署名データ$SIG_{G2,SP}$，$SIG_{G3,SP}$，$SIG_{G4,SP}$を作成する。ここで、署名データ$SIG_{G2,SP}$はコンテンツファイルＣＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{G3,SP}$はキーファイルＫＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{G4,SP}$はプライスタグデータ３１２の作成者および送信者の正当性を検証するために用いられる。

【０３３５】次に、サービスプロバイダ３１０は、図８７（Ａ）～（Ｄ）に示すように、コンテンツファイルＣＦおよびその署名データ$SIG_{8,GP}$，$SIG_{G2,SP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,GP}$，$SIG_{G3,ESG}$と、プライスタグデータ３１２およびその署名データ$SIG_{G4,SP}$と、公開鍵証明書データ$CERSP$およびその署名データ$SIG_{G1,ESG}$と、公開鍵証明書データ$CERGP$およびその署名データ$SIG_{1,ESG}$とを格納したセキュアコンテナ３０４を作成し、セキュアコンテナデポベースに格納される。セキュアコンテナデータベースに格納されたセキュアコンテナ３０４は、例えば、コンテンツＩＤなどを用いてサービスプロバイダ３１０によって一元的に管理される。なお、図８７（Ａ）は、コンテンツデータＣを伸長する ＡＶ圧縮伸長用装置として、ＤＳＰ(Digital Signal Processor)を用いた場合のコンテンツファイルＣＦの構成である。当該ＤＳＰでは、セキュアコンテナ３０４内のＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ１０４内のコンテンツデータＣの伸長および電子透かし情報の埋め込み および検出を行う。そのため、コンテンツプロバイダ３０１は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。ＡＶ圧縮伸長用装置として ＡＶ伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルＣＦ内に ＡＶ伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【０３３６】＜ステップＳ８６－４＞サービスプロバイダ３１０は、ユーザホームネットワーク３０３からの要求に応じたセキュアコンテナ３０４をセキュアコンテナデータベースから読み出す。このとき、セキュアコンテナ３０４は、複数のコンテンツファイルＣＦと、それらにそれぞれ対応した複数のキーファイルＫＦとを格納した宿舎コンテナであってもよい。例えば、単数のセキュアコンテナ３０４内に、それぞれ、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルＣＦを単数のセキュアコンテナ３０４に格納してもよい。これらの複数のコンテンツファイルＣＦなどは、ディレクトリー構造でセキュアコンテナ３０４内に格納してもよい。

【０３３７】また、セキュアコンテナ３０４は、デジタル放送で送信される場合には、ＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language) プロトコルが用いられる。このとき、セキュアコンテナ３０４内のコンテンツファイルＣＦおよびキーファイルＫＦなどは、ＭＨＥＧおよびＨＴＭＬのプロトコ

ルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ３１０とユーザホームネットワーク３０３との間で採用される通信プロトコル内の所定の階層に格納される。

【０３３８】例えば、セキュアコンテナ３０４をデジタル放送で送信する場合には、図８８に示すように、コンテンツファイルCF が、MHEGオブジェクト(Object)内のMHEGコンテンツデータとして格納される。また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES(Packetized Elementary Stream)－Videoに格納され、音声である場合にはPES－Audioに格納され、静止画である場合にはPrivate－Dataに格納される。また、図８９に示すように、キーファイルKF、プライスタグデータ３１２および公開鍵証明書データCERCP、CERSPは、トランスポート層プロトコルのTS Packet内のECM(Entitlement Control Message)に格納される。ここで、コンテンツファイルCF、キーファイルKF、プライスタグデータ３１２および公開鍵証明書データCERCP、CERSPは、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSD1 によって相互間のリンクが確立されている。

【０３３９】次に、サービスプロバイダ３１０は、セキュアコンテナ３０４を、オフラインおよび／またはオンラインでユーザホームネットワーク３０３に供給する。サービスプロバイダ３１０は、セキュアコンテナ３０４をオンラインでユーザホームネットワーク３０３のネットワーク機器３６０1 に配信する場合には、相互認証後に、セッション鍵データKSES を用いてセキュアコンテナ３０４を暗号化した後に、ネットワークを介してネットワーク機器３６０1 に配信する。

【０３４０】なお、サービスプロバイダ３１０は、セキュアコンテナ３０４を例えば衛星などを介して放送する場合には、セキュアコンテナ３０４をスクランブル鍵データKSCR を用いて暗号化する。また、スクランブル鍵データKSCR をワーク鍵データKW を暗号化し、ワーク鍵データKW をマスタ鍵データKM を用いて暗号化する。そして、サービスプロバイダ３１０は、セキュアコンテナ３０４と共に、スクランブル鍵データKSCR およびワーク鍵データKW を、衛星を介してユーザホームネットワーク３０３に送信する。また、例えば、マスタ鍵データKM を、ICカードなどに記憶してオフラインでユーザホームネットワーク３０３に配給する。

【０３４１】また、サービスプロバイダ３１０は、ユーザホームネットワーク３０３から、当該サービスプロバイダ３１０が配給したコンテンツデータCに関してのSP用購入履歴データ３０９を受信すると、これを格納する。サービスプロバイダ３１０は、将来のサービス内容を決定する際に、SP用購入履歴データ３０９を参照する。また、サービスプロバイダ３１０は、SP用購入履歴データ３０９に基づいて、当該SP用購入履歴データ３０９を送信したSAM３０５1 ～３０５4 のユーザの嗜好を分析してユーザ嗜好フィルタデータ９００を生成し、これをユーザホームネットワーク３０３のCAモジュール３１１に送信する。

【０３４２】また、サービスプロバイダ３１０の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ３０２に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。

【０３４３】また、サービスプロバイダ３１０は、EMDサービスセンタ３０２にプライスタグデータ３１２を登録して権威化してる。

【０３４４】【EMDサービスセンタ３０２】EMDサービスセンタ３０２は、前述したように、認証局（CA:CertificateAuthority）、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。図９０は、EMDサービスセンタ３０２の主な機能を示す図である。図９０に示すように、EMDサービスセンタ３０２は、主に、ライセンス鍵データをコンテンツプロバイダ３０１およびSAM３０５1 ～３０５4 に供給する処理と、公開鍵証明書データCERCP、CERSP、CERSAM1～CERSAM4の発行処理と、キーファイルKFの発行処理、利用履歴データ３０８に基づいた決済処理（利益分配処理）とを行う。ここで、ライセンス鍵データの供給処理と、公開鍵証明書データCERCP、CERSAM1～CERSAM4の発行処理と、キーファイルKFの生成処理とは、第１実施形態のEMDサービスセンタ１０２と同じである。

【０３４５】EMDサービスセンタ３０２は、EMDサービスセンタ１０２とは異なり、さらにサービスプロバイダ３１０の公開鍵証明書データCERSP の発行処理を行う。また、EMDサービスセンタ３０２は、利用履歴データ３０８に基づいて、SAM３０５1 ～３０５4 におけるコンテンツデータCの購入によって支払われた利益をコンテンツプロバイダ３０１およびサービスプロバイダ３１０の関係者に分配する利益分配処理を行う。ここで、利用履歴データ３０８の内容は、例えば図２１に示される。

【０３４６】また、EMDサービスセンタ３０２は、利用履歴データ３０８に基づいて、当該利用履歴データ３０８を送信したSAM３０５1 ～３０５4 のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ９０３を生成し、ユーザ嗜好フィルタデータ９０３をSAM管理部１４９を介して、当該利用履歴データ３０８を送信したSAM３０５1 ～３０５4 に送信する。

【０３４７】【ユーザホームネットワーク３０３】ユーザホームネットワーク３０３は、図８５に示すように、ネットワーク機器３６０1 およびA／V機器３６０2 ～

３６０４を有している。ネットワーク機器３６０１は、ＣＡモジュール３１１およびＳＡＭ３０５１を内蔵している。また、ＡＶ機器３６０２～３６０４は、それぞれＳＡＭ３０５２～３０５４を内蔵している。ＳＡＭ３０５１～３０５４の相互間は、例えば、１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。なお、ＡＶ機器３６０２～３６０４は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器３６０１のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク３０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０３４８】以下、ネットワーク機器３６０１について説明する。図９１は、ネットワーク機器３６０１の構成図である。図９１に示すように、ネットワーク機器３６０１は、通信モジュール１６２、ＣＡモジュール３１１、復号モジュール９０５、ＳＡＭ３０５１、ＡＶ圧縮・伸長用ＳＡＭ１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。図９１において、図２２と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。

【０３４９】通信モジュール１６２は、サービスプロバイダ３１０との間の通信処理を行なう。具体的には、通信モジュール１６２は、サービスプロバイダ３１０から衛星放送などで受信したセキュアコンテナ３０４を復号モジュール９０５に出力する。また、通信モジュール１６２は、サービスプロバイダ３１０から電話回線などを介して受信したユーザ嗜好フィルタデータ９００をＣＡモジュール３１１に出力すると共に、ＣＡモジュール３１１から入力したＳＰ用購入履歴データ３０９を電話回線などを介してサービスプロバイダ３１０に送信する。

【０３５０】図９２は、ＣＡモジュール３１１および復号モジュール９０５の機能ブロック図である。図９２に示すように、ＣＡモジュール３１１は、相互認証部９０６、記憶部９０７、暗号化・復号部９０８およびＳＰ用購入履歴データ生成部９０９を有する。相互認証部９０６は、ＣＡモジュール３１１とサービスプロバイダ３１０との間で電話回線を介してデータを送受信する際に、サービスプロバイダ３１０との間で相互認証を行ってセッション鍵データＫｓｅｓを生成し、これを暗号化・復号部９０８に出力する。

【０３５１】記憶部９０７は、例えば、サービスプロバイダ３１０とユーザとの間で契約が成立した後に、サービスプロバイダ３１０からＩＣカード９１２などを用いてオフラインで供給されたマスタ鍵データＫｍを記憶する。

【０３５２】暗号化・復号部９０８は、復号モジュール９０５の復号部９１０からそれぞれ暗号化されたスクランブル鍵データＫｓｃｒおよびワーク鍵データＫｗを入力し、記憶部９０７から読み出したマスタ鍵データＫｍを用いてワーク鍵データＫｗを復号する。そして、暗号化・復号部９０８は、当該復号したワーク鍵データＫｗを用いてスクランブル鍵データＫｓｃｒを復号し、当該復号したスクランブル鍵データＫｓｃｒを復号部９１０に出力する。また、暗号化・復号部９０８は、電話回線などを介して通信モジュール１６２がサービスプロバイダ３１０から受信したユーザ嗜好フィルタデータ９００を、相互認証部９０６からのセッション鍵データＫｓｅｓを用いて復号して復号モジュール９０５のセキュアコンテナ選択部９１１に出力する。また、暗号化・復号部９０８は、ＳＰ用購入履歴データ生成部９０９から入力したＳＰ用購入履歴データ３０９を、相互認証部９０６からのセッション鍵データＫｓｅｓを用いて復号して通信モジュール１６２を介してサービスプロバイダ３１０に送信する。

【０３５３】ＳＰ用購入履歴データ生成部９０９は、図９１に示す購入・利用形態決定操作部１６５を用いてユーザによるコンテンツデータＣの購入操作に応じた操作信号Ｓ１６５、またはＳＡＭ３０５１からの利用制御データ１６６に基づいて、サービスプロバイダ３１０に固有のコンテンツデータＣの購入履歴を示すＳＰ用購入履歴データ３０９を生成し、これを暗号化・復号部９０８に出力する。ＳＰ用購入履歴データ３０９は、例えば、サービスプロバイダ３１０が配信サービスに関してユーザから徴収した情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【０３５４】なお、ＣＡモジュール３１１は、サービスプロバイダ３１０が課金機能を有している場合には、サービスプロバイダ３１０の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、ＣＡモジュール３１１は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ３１０に送信する。

【０３５５】復号モジュール９０５は、復号部９１０およびセキュアコンテナ選択部９１１を有する。復号部９１０は、通信モジュール１６２から、それぞれ暗号化されたセキュアコンテナ３０４、スクランブル鍵データＫｓｃｒおよびワーク鍵データＫｗを入力する。そして、復号部９１０は、暗号化されたスクランブル鍵データＫｓｃｒおよびワーク鍵データＫｗをＣＡモジュール３１１の暗号化・復号部９０８に出力し、暗号化・復号部９０８から復号されたスクランブル鍵データＫｓｃｒを入力する。そして、復号部９１０は、暗号化されたセキュアコンテナ３０４を、スクランブル鍵データＫｓｃｒを用いて復号した後に、セキュアコンテナ選択部９１１に出力する。

【０３５６】なお、セキュアコンテナ３０４が、MPEG2

Transport Stream 方式でサービスプロバイダ３１０から送信される場合には、例えば、復号部９１０は、ＩＳＰacket 内のＥＣＭ(Entitlement Control Message) からスクランブル鍵データK_{scr}を取り出し、ＥＭＭ(Entitlement Management Message)からワーク鍵データK_wを取り出す。ＥＣＭには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ＥＭＭは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【０３５７】セキュアコンテナ選択部９１１は、復号部９１０から入力したセキュアコンテナ３０４を、ＣＡモジュール３１１から入力したユーザ嗜好フィルタデータ９００を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ３０４を選択してＳＡＭ３０５$_1$に出力する。

【０３５８】次に、ＳＡＭ３０５$_1$について説明する。なお、ＳＡＭ３０５$_1$は、サービスプロバイダ３１０についての署名検証処理を行なうなど、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０に関しての処理を行う点を除いて、図２２～図６１などを用いて前述した第１実施形態のＳＡＭ１０５$_1$と基本的に行なう機能および構造を有している。ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ３０２との間で通信を行う。

【０３５９】また、図６２に示す構成はユーザホームネットワーク３０３内の機器においても適用可能である。また、図６３～図８２を用いて説明した権利処理用のＳＡＭ、メディアＳＡＭ１３３、ＡＶＥ綿・伸長用ＳＡＭ１６３およびメディア・ドラブＳＡＭ２６０の構成は、ユーザホームネットワーク３０３内の機器で用いられる各種のＳＡＭにも適用される。また、ＳＡＭ３０５$_2$～３０５$_4$は、ＳＡＭ３０５$_1$と基本的に同じ機能を有

【０３６０】以下、ＳＡＭ３０５$_1$の機能について詳細に説明する。図９３は、ＳＡＭ３０５$_1$の機能の構成図である。なお、図９３には、サービスプロバイダ３１０からセキュアコンテナ３０４を入力する際の処理に関連するデータの流れが示されている。図９３に示すように、ＳＡＭ３０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、ダウンロードメモリ管理部１８２、ＡＶＥ綿・伸長用ＳＡＭ管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、ＳＡＭ管理部１９０、記憶部１９２、メディアＳＡＭ管理部１９７、作業用メモリ２００、サービスプロバイダ管理部５８０、課金処理部５８７、署名処理部５８９および外部メモリ管理部８１１を有する。なお、図９３に示すＳＡＭ３０５$_1$の所定の機能は、ＳＡＭ１０５$_1$の場合と同様に、ＣＰＵにおいて秘密プログラムを実行することによって実現される。図９３において、図２３等と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと同じである。ここで、コンテンツプロバイダ管理部１８０およびダウンロードメモリ管理部１８２が本発明の入力処理手段に対応し、課金処理部５８７が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部１７２が本発明の復号手段に対応し、利用監視部１８６が本発明の利用制御手段に対応している。また、暗号化・復号部１７３が本発明の暗号化手段に対応している。また、後述する例えば図９１に示すメディア・ドライブＳＡＭ管理部８５５が本発明の記録制御手段に対応している。また、署名処理部１８９が本発明の署名処理手段に対応している。

【０３６１】また、図９１に示す外部メモリ２０１には、第１実施形態で説明した処理および後述する処理を経て、利用履歴データ３０８およびＳＡＭ登録リストが記憶される。また、作業用メモリ２００には、図９４に示すように、コンテンツ鍵データK_c、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOS}、コンテンツプロバイダ３０１の公開鍵証明書データCER_{SP}、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}、利用制御データ（ＵＣＳ）３６６、ＳＡＭプログラム・ダウンロード・コンテンツSDC_1～SDC_3およびプライスタグデータ３１２などが記憶される。

【０３６２】以下、ＳＡＭ３０５$_1$の機能ブロックのうち、図９３において新たに符号を付した機能ブロックについて説明する。署名処理部５８９は、記憶部１９２あるいは作業用メモリ２００から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$、コンテンツプロバイダ３０１の公開鍵データ$K_{SDP,P}$およびサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、セキュアコンテナ３０４内の署名データの検証を行なう。

【０３６３】課金処理部５８７は、図９５に示すように、図９１に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５と、作業用メモリ２００から読み出されたプライスタグデータ３１２とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。なお、プライスタグデータ３１２は、ユーザがコンテンツデータの購入形態等を決定する際に、所定の出力手段を介してＳＡＭ３０５$_1$の外部に出力され、コンテンツデータの販売価格をユーザに表示等するために用いられる。課金処理部５８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【０３６４】また、課金処理部５８７は、課金処理において、利用履歴データ３０８を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。

ここで、利用履歴データ３０８は、第１実施形態の利用履歴データ１０８と同様に、ＥＭＤサービスセンタ３０２において、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。

【０３６５】また、課金処理部５８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態（UCS: Usage Control Status）データ１６６を生成し、これを作業用メモリ２００に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ１６６には、コンテンツのＩＤ、購入形態、買い切り価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０３６６】なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ３０５ｉからサービスプロバイダ３１０に利用制御データ１６６をリアルタイムに送信し、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２に、利用履歴データ３０８をＳＡＭ１０５ｉに取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ１６６が、サービスプロバイダ３１０およびＥＭＤサービスセンタ３０２にリアルタイムに送信される。

【０３６７】また、ＳＡＭ３０５ｉでは、図９３に示すように、ＥＭＤサービスセンタ管理部１８５を介してＥＭＤサービスセンタ３０２から受信したユーザ嗜好フィルタデータ９０３が、サービスプロバイダ管理部５８０に出力される。そして、サービスプロバイダ管理部５８０において、図９１に示す復号モジュール９０５から入力したセキュアコンテナ３０４のうち、ユーザ嗜好フィルタデータ９０３に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ３０４が選択され、当該選択されたセキュアコンテナ３０４がダウンロードメモリ管理部１８２に出力される。これにより、ＳＡＭ３０５ｉにおいて、当該ＳＡＭ３０５ｉのユーザが契約している全てのサービスプロバイダ３１０を対象として、当該ユーザによるコンテンツデータＣの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータＣの選択処理が可能になる。

【０３６８】以下、ＳＡＭ３０５ｉ内での処理の流れを説明する。

＜ライセンス鍵データの受信時の処理＞ＥＭＤサービスセンタ３０２から受信したライセンス鍵データＫＤ１～ＫＤｓを記憶部１９２に格納する際のＳＡＭ３０５ｉ内での処理の流れは、図２８を用いて前述した第１実施形態のＳＡＭ１０５ｉの場合と同様である。

【０３６９】＜セキュアコンテナ３０４をサービスプロバイダ３１０から入力した時の処理＞次に、セキュアコンテナ３０４をサービスプロバイダ３１０から入力する際のＳＡＭ３０５ｉ内での処理の流れを図９６を参照しながら説明する。なお、以下に示す例では、ＳＡＭ１０５ｉにおいて、セキュアコンテナ１０４を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ１０４の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップＳ９６－１：図９３に示すＳＡＭ３０５ｉの相互認証部１７０とサービスプロバイダ３１０との間で相互認証を行なう。

ステップＳ９６－２：ＳＡＭ３０５ｉの相互認証部１７０とダウンロードメモリ１６７のメディアＳＡＭ１６７ａとの間で相互認証を行なう。

【０３７０】ステップＳ９６－３：サービスプロバイダ３１０から受信したセキュアコンテナ３０４を、ダウンロードメモリ１６７に書き込む。このとき、ステップＳ９６－２で得られたセッション鍵データを用いて、相互認証部１７０におけるセキュアコンテナ３０４の署名化と、メディアＳＡＭ１６７ａにおけるセキュアコンテナ３０４の復号とを行なう。

ステップＳ９６－４：ＳＡＭ３０５ｉは、ステップＳ９６－１で得られたセッション鍵データを用いて、セキュアコンテナ３０４の復号を行なう。

【０３７１】ステップＳ９６－５：署名処理部５８９は、図８７（Ｄ）に示す署名データＳＩ$_{G61,ESC}$の検証を行なった後に、図８７（Ｄ）に示す公開鍵証明書データＣＥＲ$_{RSP}$内に格納されたサービスプロバイダ３１０の公開鍵データＫ$_{SP,P}$を用いて、署名データＳＩ$_{G62,SP}$，ＳＩ$_{G63,SP}$，ＳＩ$_{G64,SP}$の正当性を検証する。このとき、署名データＳＩ$_{G62,SP}$が正当であると検証されたときに、コンテンツファイルＣＦの送信者の正当性が確認される。署名データＳＩ$_{G63,SP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。署名データＳＩ$_{G64,SP}$が正当であると検証されたときに、プライスタグデータ３１２の作成者および送信者の正当性が確認される。

【０３７２】ステップＳ９６－６：署名処理部５８９は、図８７（Ｄ）に示す署名データＳＩ$_{G1,ESC}$の検証を行なった後に、図８７（Ｃ）に示す公開鍵証明書データＣＥＲ$_{CP}$内に格納されたコンテンツプロバイダ３０１の公開鍵データＫ$_{CP,P}$を用いて、署名データＳＩ$_{G8,CP}$，ＳＩ$_{G7,CP}$の正当性を検証する。このとき、署名データＳＩ$_{G8,CP}$が正当であると検証されたときに、コンテンツファイルＣＦの作成者および送信者の正当性が確認される。また、署名データＳＩ$_{G7,CP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正

当性が確認される。

【０３７３】ステップＳ９６－７：署名処理部５８９は、記憶部１９２から読み出した公開鍵データ$K_{ESE,P}$を用いて、図８７（Ｂ）に示すキーファイルＫＦ内の署名データＳＩＧ$_{KI,ESD}$の正当性、すなわちキーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２に登録されているか否かの検証を行う。

【０３７４】ステップＳ９６－８：暗号化・復号部１７２は、記憶部１９２から読み出した対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_3$を用いて、図８７（Ｂ）に示すキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$を復号し、これらを作業用メモリ２００に書き込む。

【０３７５】＜ダウンロードしたセキュアコンテナの購入形態決定処理＞ダウンロードしたセキュアコンテナの購入形態決定処理は、基本的に、第１実施形態において、図３１を用いて前述したＳＡＭ１０５$_1$の場合と同じである。当該購入形態決定処理により、後述する図１００（Ｃ）に示すキーファイルＫＦ$_1$が作業用メモリ２００およびダウンロードメモリ管理部１８２を介してダウンロードメモリ１６７に記憶される。

【０３７６】＜コンテンツデータの再生処理＞ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣの再生処理は、基本的に、第１実施形態において、図３３を用いて説明したＳＡＭ１０５$_1$の処理と同じである。

【０３７７】＜一の機器の利用制御データ（ＵＳＣ）１６６を使用して他の機器で再購入を行う場合の処理＞先ず、図９７に示すように、例えば、ネットワーク機器３６０$_1$のダウンロードメモリ１６７にダウンロードされたコンテンツファイルＣＦの購入形態を前述したように決定した後に、当該コンテンツファイルＣＦを格納した新たなセキュアコンテナ３０４ｘを生成し、バス１９１を介して、ＡＶ機器３６０$_2$のＳＡＭ３０５$_2$にセキュアコンテナ３０４ｘを転送するまでのＳＡＭ１０５$_1$内での処理の流れを図９８および図９９を参照しながら説明する。

【０３７８】図９９は、当該処理のフローチャートである。図９９に示す処理を行う前提として、前述した購入処理によって、ＳＡＭ３０５$_1$の作業用メモリ２００には図１００（Ｃ）に示すキーファイルＫＦ$_1$およびそのハッシュ値Ｈ$_{K1}$が記憶されている。

ステップＳ９９－１：ユーザは、図９１および図９７に示すに購入・利用形態決定操作部１６５を操作して、購入形態を既に決定したセキュアコンテナをＳＡＭ３０５$_2$に転送することを指示する。課金処理部５８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ３０８を更新する。

【０３７９】ステップＳ９９－２：ＳＡＭ３０５$_1$は、第１実施形態で前述したＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ３０５$_2$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ９６－３以降の処理を行う。また、ＳＡＭ１０５$_1$は、ＳＡＭ１０５$_2$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０３８０】ステップＳ９９－３：相互認証部１７０は、ＳＡＭ３０５$_2$との間で相互認証を行って得たセッション鍵データK_{SES}を共有する。

【０３８１】ステップＳ９９－４：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図８７（Ａ）に示すコンテンツファイルＣＦおよび署名データＳＩＧ$_{G4.CP}$，ＳＩＧ$_{G2.SP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データK_{SANI}を用いた署名データＳＩＧ$_{41,SAN1}$を署名処理部１８９に作成させる。

【０３８２】ステップＳ９９－５：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図８７（Ｂ）に示すキーファイルＫＦおよび署名データＳＩＧ$_{7.CP}$，ＳＩＧ$_{63.SP}$を読み出し、これについてのＳＡＭ３０５$_1$の秘密鍵データK_{SANI}を用いた署名データＳＩＧ$_{42.SAN1}$を署名処理部５８９に作成させる。

【０３８３】ステップＳ９９－６：ＳＡＭ管理部１９０は、図１００に示すセキュアコンテナ３０４ｘを作成する。

ステップＳ９９－７：暗号化・復号部１７１において、ステップＳ９６－３で得たセッション鍵データK_{SES}を用いて、図１００に示すセキュアコンテナ３０４ｘが暗号化される。

【０３８４】ステップＳ９９－８：ＳＡＭ管理部１９０は、セキュアコンテナ３０４ｘを図９７に示すＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に出力する。このとき、ＳＡＭ３０５$_1$とＳＡＭ３０５$_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０３８５】以下、図９７に示すように、ＳＡＭ３０５$_1$から入力した図１００に示すセキュアコンテナ３０４ｘを、ＲＡＭ型などの記録媒体（メディア）１３０$_4$に書き込む際のＳＡＭ３０５$_2$内での処理の流れを図１０１，図１０２および図１０３を参照して説明する。図１０２および図１０３は、当該処理を示すフローチャートである。ここで、ＲＡＭ型の記録媒体１３０$_4$は、例えば、セキュアでないＲＡＭ領域１３４、メディアＳＡＭ１３３およびセキュアＲＡＭ領域１３２を有している。

【０３８６】ステップＳ１０２－１：ＳＡＭ３０５$_2$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送元のＳＡＭ３０５$_1$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ９９－２以降の処理を行う。また、

ＳＡＭ３０５$_{2}$は、ＳＡＭ３０５$_{1}$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０３８７】ステップＳ１０２－２：前述したステップＳ９９－３に対応する処理として、ＳＡＭ３０５$_{2}$は、ＳＡＭ３０５$_{1}$との間で相互認証を行って得たセッション鍵データK_{SES}を共有する。

ステップＳ１０２－３：ＳＡＭ３０５$_{2}$のＳＡＭ管理部１９０は、図９７に示すように、ネットワーク機器３６０）のＳＡＭ３０５$_{1}$からセキュアコンテンツ３０４ｘを入力する。

ステップＳ１０２－４：暗号化・復号部１７１は、ステップＳ９９－２で共有したセッション鍵データK_{SES}を用いて、ＳＡＭ管理部１９０を介して入力したセキュアコンテンツ３０４ｘを復号する。

【０３８８】ステップＳ１０２－５：セッション鍵データK_{SES}を用いて復号されたセキュアコンテンツ３０４ｘ内のコンテンツファイルＣＦが、図９７に示すメディア・ドラブＳＡＭ２６０におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体１３０４のＲＡＭ領域１３４に記録される。

【０３８９】ステップＳ１０２－６：セッション鍵データK_{SES}を用いて復号されたセキュアコンテンツ３０４ｘ内の署名データＳＩＧ$_{G6.CP}$，ＳＩＧ$_{G2.SP}$，ＳＩＧ$_{41.SAM1}$と、キーファイルＫＦおよびその署名データＳＩＧ$_{7.CP}$，，ＳＩＧ$_{63.SP}$，ＳＩＧ$_{42.SAM1}$と、キーファイルＫＦ$_{1}$およびそのハッシュ値H_{K1}と、公開鍵署名データＣＥＲ$_{SP}$およびその署名データＳＩＧ$_{61.ESG}$と、公開鍵署名データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1.ESG}$と、公開鍵署名データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22.ESG}$とが、作業用メモリ２００に書き込まれる。

【０３９０】ステップＳ１０２－７：署名処理部５８９において、作業用メモリ２００から読み出された署名データＳＩＧ$_{61.ESG}$，ＳＩＧ$_{1.ESG}$，ＳＩＧ$_{22.ESG}$が、記憶部１９２から読み出した公開鍵データ$K_{ESG.P}$を用いて検証され、公開鍵証明書データＣＥＲ$_{SP}$，ＣＥＲ$_{CP}$，ＣＥＲ$_{SAM1}$の正当性が確認される。そして、署名処理部５８９において、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データ$K_{CP.P}$を用いて、署名データＳＩＧ$_{6.CP}$の正当性が検証され、コンテンツファイルＣＦの作成者の正当性が確認される。署名処理部５８９において、公開鍵証明書データＣＥＲ$_{SP}$に格納された公開鍵データ$K_{SP.P}$を用いて、署名データＳＩＧ$_{62.CP}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。また、署名処理部１８９において、公開鍵証明書データＣＥＲ$_{SAM1}$に格納された公開鍵データ$K_{SAM1.P}$を用いて、署名データＳＩＧ$_{41.SAM1}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。

【０３９１】ステップＳ１０２－８：署名処理部５８９において、公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$，ＣＥＲ$_{SAM1}$に格納された公開鍵データ$K_{CP.P}$，$K_{SP.P}$，$K_{SAM1.P}$を用いて、作業用メモリ２００に記憶されている署名データＳＩＧ$_{7.CP}$，ＳＩＧ$_{63.SP}$，ＳＩＧ$_{42.SAM1}$の正当性を検証する。そして、署名データＳＩＧ$_{7.CP}$，ＳＩＧ$_{63.SP}$，ＳＩＧ$_{42.SAM1}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０３９２】ステップＳ１０２－９：署名処理部１８９において、記憶部１９２から読み出した公開鍵データ$K_{ESG.P}$を用いて、図１００（Ｂ）のキーファイルＫＦに格納されが署名データＳＩＧ$_{K1.ESG}$の検証が行われる。そして、署名データＳＩＧ$_{K1.ESG}$が正当であると検証されたときに、キーファイルＫＦの作成者の正当性が確認される。

【０３９３】ステップＳ１０２－１０：署名処理部１８９は、ハッシュ値H_{K1}の正当性を検証し、キーファイルＫＦ$_{1}$の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルＫＦ$_{1}$の作成者と送信元とが同じ場合を述べたが、キーファイルＫＦ$_{1}$の作成者と送信元とが異なる場合には、キーファイルＫＦ$_{1}$に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０３９４】ステップＳ１０２－１１：利用監視部１８５は、ステップＳ９９－１０で復号されたキーファイルＫＦ$_{1}$に格納された利用制御データ１６６を用いて、以後のコンテンツデータＣの購入・利用形態を制御する。

【０３９５】ステップＳ１０２－１２：ユーザは、購入・利用形態決定操作部１６５を操作して購入形態を決定し、当該操作に応じた操作信号Ｓ１６５が、課金処理部５８７に出力される。

ステップＳ１０２－１３：課金処理部５８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ３０８を更新する。また、課金処理部５８７は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ１６６を更新する。

【０３９６】ステップＳ１０２－１４：暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR}，メディア鍵データK_{MED}および購入者鍵データK_{PIN}を鍵に用いて、ステップＳ９９－１２で生成された利用制御データ１６６を暗号化してメデディア・ドライブＳＡＭ管理部８５５に出力する。

ステップＳ１０２－１５：メディア・ドライブＳＡＭ管理部８５５は、新たな利用制御データ１６６を格納したキーファイルＫＦ$_{1}$を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処

理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体１３０₄のセキュアＲＡＭ領域１３２に記録する。

ステップＳ１０２－１６：キーファイルＫＦが作業用メモリ２００から読み出され、メディア・ドライブＳＡＭ管理部８５５を介して、図９７に示すメディア・ドラブＳＡＭ２６０によってＲＡＭ型の記録媒体１３０₄のセキュアＲＡＭ領域１３２に書き込まれる。

【０３９７】なお、ＳＡＭ３０５₁におけるＲＯＭ型の記録媒体のコンテンツデータの購入形態決定処理、ＲＯＭ型の記録媒体のコンテンツデータの購入形態を決定した後にＲＡＭ型の記録媒体に書き込む場合の処理は、サービスプロバイダ３１０において秘密鍵データ$K_{SP.P}$を用いて付けられた署名データＳＩＧ$_{SP}$の検証処理を行う点を除いて、前述した第１実施形態のＳＡＭ１０５₁における処理と同じである。また、ＳＡＭ３０５₁の実現方法も、前述した第１実施形態で説明したＳＡＭ１０５₁の実現方法と同じである。また、ユーザホームネットワーク３０３に用いられる機器においても、第１実施形態で説明した図６２に示す構成は同様に適用される。また、この場合に、ＳＡＭ３０５₁、ＡＶ圧縮・伸長用ＳＡＭ１６３、メディア・ドラブＳＡＭ２６０およびメディアＳＡＭ１３３の回路モジュールとして、図６３～図８２を用いて説明した構成が同様に適用される。また、図５７～図６１を用いて説明したセキュア機能も、コンテンツプロバイダ１０１がサービスプロバイダ３１０に置き換える点を除いて、ＥＭＤシステム３００でも同様に適用される。

【０３９８】以下、ユーザホームネットワーク３０３における各種の機器の接続形態等を再び説明する。図１０４は、ユーザホームネットワーク３０３における機器の接続形態の一例を説明するための図である。ここでは、図１０４に示すように、ユーザホームネットワーク３０３内でネットワーク機器３６０₁，ＡＶ機器３６０₂，３６０₃がＩＥＥＥ１３９４シリアルバス１９１を介して接続されている場合を説明する。ネットワーク機器３６０₁は、外部メモリ２０１、ＳＡＭ３０５₁、ＣＡモジュール３１１、ＡＶ圧縮・伸長用ＳＡＭ１６３およびダウンロードメモリ１６７を有する。ＣＡモジュール３１１は、公衆回線などのネットワークを介して、サービスプロバイダ３１０と通信を行う。また、ＳＡＭ３０５₁は、公衆回線などのネットワークを介して、ＥＭＤサービスセンタ３０２と通信を行う。ダウンロードメモリ１６７としては、メディアＳＡＭ１６７$_a$を備えたメモリスティック、あるいはＨＤＤなどが用いられる。ダウンロードメモリ１６７には、サービスプロバイダ３１０からダウンロードしたセキュアコンテナ３０４などが記憶される。各機器には、ＡＴＲＡＣ３やＭＰＥＧなどの各種の圧縮・伸長方式にそれぞれ対応した複数のＡＶ圧縮・伸長用ＳＡＭ１６３が内蔵されている。ＳＡＭ３０５₁は、接触方式あるいは非接触方式のＩＣカード１１４１と通信を行うことが可能である。ＩＣカード１１４１は、ユーザＩＤなどの各種のデータが記憶しており、ＳＡＭ３０５₁においてユーザ認証を行う場合などに用いられる。

【０３９９】ＡＶ機器３６０₂は、例えば、ストレージ機器であり、ＳＡＭ３０５₂とＳＡＭ３０５₃との間で所定の処理を経て、ＩＥＥＥ１３９４シリアルバス１９１を介してネットワーク機器３６０₁から入力したセキュアコンテナを記録媒体１３０に記録する。また、ＡＶ機器３６０₃も同様に、例えば、ストレージ機器であり、ＳＡＭ３０５₂とＳＡＭ３０５₃との間で所定の処理を経て、ＩＥＥＥ１３９４シリアルバス１９１を介してＡＶ機器３６０₃から入力したセキュアコンテナを記録媒体１３０に記録する。

【０４００】なお、図１０４に示す例では、記録媒体１３０にメディアＳＡＭ１３３が搭載されている場合を例示したが、例えば、記録媒体１３０のメディアＳＡＭ１３３が搭載されていない場合には、図１０４に点線で示したように、メディア・ドラブＳＡＭ２６０を用いて、ＳＡＭ３０５₂，３０５₃との間の認証が行われる。

【０４０１】次に、図８５に示すＥＭＤシステム３００の全体動作について説明する。図１０５および図１０６は、ＥＭＤシステム３００の全体動作のフローチャートである。ここでは、サービスプロバイダ３１０からユーザホームネットワーク３０３にオンラインでセキュアコンテナ３０４を送信する場合を例示して説明する。なお、以下に示す処理の前提として、ＥＭＤサービスセンタ３０２へのコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５₁～３０５₄の登録は既に終了しているものとする。

【０４０２】ステップＳ２１：ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{CP.P}$の公開鍵証明書CER_{CP}を、自らの署名データＳＩＧ$_{1.ESC}$と共にコンテンツプロバイダ３０１に送信する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{SP.P}$の公開鍵証明書CER_{SP}を、自らの署名データＳＩＧ$_{61.ESC}$と共にサービスプロバイダ３１０に送信する。また、ＥＭＤサービスセンタ３０２は、各々有効期限が１カ月の３カ月分のライセンス鍵データＫＤ₁～ＫＤ₃をユーザホームネットワーク３０３のＳＡＭ３０５₁～３０５₄に送信する。

【０４０３】ステップＳ２２：コンテンツプロバイダ３０１は、相互認証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃをＥＭＤサービスセンタ３０２に登録して権威化する。また、ＥＭＤサービスセンタ３０２は、図３（Ｂ）に示す６カ月分のキーファイルＫＦを作成し、これをコンテンツプロバイダ３０１に送信する。

【０４０４】ステップＳ２３：コンテンツプロバイダ３

０１は、図３（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データＳＩＧ6,CP と、キーファイルＫＦおよびその署名データＳＩＧ7,CP とを作成し、これらと図３（Ｃ）に示す公開鍵証明書データＣＥＲCP および署名データＳＩＧ1,ESC とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、サービスプロバイダ３１０に提供する。

【０４０５】ステップＳ２４：サービスプロバイダ３１０は、図３（Ｃ）に示す署名データＳＩＧ1,ESC を検証した後に、公開鍵証明書データＣＥＲCP に格納された公開鍵データＫCP,P を用いて、図３（Ａ），（Ｂ）に示す署名データＳＩＧ6,CP およびＳＩＧ7,CP を検証して、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１から送信されたものであるかを確認する。

【０４０６】ステップＳ２５：サービスプロバイダ３１０は、プライスタグデータ３１２およびその署名データＳＩＧ64,SP を作成し、これらを格納したを格納した図６５に示すセキュアコンテナ３０４を作成する。

【０４０７】ステップＳ２６：サービスプロバイダ３１０は、プライスタグデータ３１２をＥＭＤサービスセンタ３０２に逆鍵して確鍵化する。

【０４０８】ステップＳ２７：サービスプロバイダ３１０は、例えば、ユーザホームネットワーク３０３のＣＡモジュール３１１からの要求に応じて、ステップＳ２５で作成したセキュアコンテナ３０４を、オンラインあるいはオフラインで、図７４に示すネットワーク機器３６０１の復号モジュール９０５に送信する。

【０４０９】ステップＳ２８：ＣＡモジュール３１１は、ＳＰ用簿入履歴データ３０９を作成し、これを所定のタイミングで、サービスプロバイダ３１０に送信する。

【０４１０】ステップＳ２９：ＳＡＭ３０５1 ～３０５4 のいずれかにおいて、図８７（Ｄ）に示す署名データＳＩＧ61,ESC を検証した後に、公開鍵証明書データＣＥＲSP に格納された公開鍵データＫSP,P を用いて、図８７（Ａ），（Ｂ），（Ｃ）に示す署名データＳＩＧ62,SP ，ＳＩＧ63,SP ，ＳＩＧ64,SP を検証して、セキュアコンテナ３０４内の所定のデータが正当なサービスプロバイダ３１０において作成および送信されたか否かを確認する。

【０４１１】ステップＳ３０：ＳＡＭ３０５1 ～３０５4 のいずれかにおいて、図８７（Ｄ）に示す署名データＳＩＧ1,ESC を検証した後に、公開鍵証明書データＣＥＲCP に格納された公開鍵データＫCP,P を用いて、図８７（Ａ），（Ｈ），（Ｃ）に示す署名データＳＩＧ6,SP，ＳＩＧ7,SP を検証して、セキュアコンテナ３０４内のコンテンツファイルＣＦが正当なコンテンツプロバイダ３０１において作成されたか否かと、キーファイルＫＦが正当なコンテンツプロバイダ３０１から送信されたか否かを確認する。また、ＳＡＭ３０５1 ～３０５4 のいず

れかにおいて、公開鍵データＫESC,P を用いて、図８７（Ｂ）に示すキーファイルＫＦ内の署名データＳＩＧK1,ESC の正当性を検証することで、キーファイルＫＦが正当なＥＭＤサービスセンタ３０２によって作成されたか否かを確認する。

【０４１２】ステップＳ３１：ユーザが図９１の購入・利用形態決定操作部１６５を操作してコンテンツの購入・利用形態を決定する。

【０４１３】ステップＳ３２：ステップＳ３１において生成された操作信号Ｓ１６５に基づいて、ＳＡＭ３０５1 ～３０５4 において、セキュアコンテナ３０４の利用履歴（Usage Log）データ３０８が生成される。ＳＡＭ３０５1 ～３０５4 からＥＭＤサービスセンタ３０２に、利用履歴データ３０８およびその署名データＳＩＧ205,SAM1 が送信される。また、購入形態が決定される度にリアルタイムに、ＳＡＭ３０５1 ～３０５4 からＥＭＤサービスセンタ３０２に利用制御状態データ１６６が送信される。

【０４１４】ステップＳ３３：ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、決済請求権データ１５２ｃ，１５２ｓを作成する。

【０４１５】ステップＳ３４：ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓを自らの署名データと共に送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者に分配される。

【０４１６】以上説明したように、ＥＭＤシステム３００では、図３に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ３０１からサービスプロバイダ３１０に配給し、セキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦをそのまま格納したセキュアコンテナ３０４をサービスプロバイダ３１０からユーザホームネットワーク３０３に配給し、キーファイルＫＦについての処理をＳＡＭ３０５1 ～３０５4 内で行う。また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データＫD1 ～ＫD3 を用いて暗号化されており、配信鍵データＫD1 ～ＫD3 を保持しているＳＡＭ３０５1 ～３０５4 内でのみ復号される。そして、ＳＡＭ３０５1 ～３０５4 では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

【０４１７】従って、ＥＭＤシステム３００によれば、ユーザホームネットワーク３０３におけるコンテンツデ

ータＣの購入および利用を、サービスプロバイダ３１０における処理とは無関係に、コンテンツプロバイダ３０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。すなわち、ＥＭＤシステム３００によれば、権利書データ１０６をサービスプロバイダ３１０が管理できないようできる。そのため、ＥＭＤシステム３００によれば、異系列の複数のサービスプロバイダ３１０を介してユーザホームネットワーク３０３にコンテンツデータＣが配給された場合でも、ユーザホームネットワーク３０３のＳＡＭにおける当該コンテンツデータＣについての権利処理を、コンテンツプロバイダ３０１が作成した共通の権利書データ１０６に基づいて行わせることができる。

【０４１８】また、ＥＭＤシステム３００では、セキュアコンテナ１０４，３０４内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ３１０およびＳＡＭ３０５１～３０５４において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータＣの不正利用を効果的に回避できる。

【０４１９】また、ＥＭＤシステム３００では、サービスプロバイダ３１０からユーザホームネットワーク３０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ３０４を用いて行うことで、双方の場合において、ＳＡＭ３０５１～３０５４におけるコンテンツデータＣの権利処理を共通化できる。

【０４２０】また、ＥＭＤシステム３００では、ユーザホームネットワーク３０３内のネットワーク機器３６０１およびＡＶ機器３６０２～３６０４においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。例えば、図１０７に示すように、コンテンツプロバイダ３０１が提供したコンテンツデータＣを、サービスプロバイダ３１０からユーザホームネットワーク３０３に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク３０３，３０３ａのＳＡＭにおいて、コンテンツプロバイダ３０１が作成した権利書データ１０６に基づいて、共通の権利処理ルールが採用される。

【０４２１】また、ＥＭＤシステム３００によれば、ＥＭＤサービスセンタ３０２が、認証機能、鍵データ管理機能および権利処理（利益分）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２の所有者に、予め決められた比率に従って確実に分配される。また、ＥＭＤシステム３００によれば、同じコンテンツプロバイダ３０１が供給した同じコンテンツファイルＣＦについての権利書データ１０６は、サービスプロバイダ３１０のサービス形態とは無関係に、そのままＳＡＭ３０５１～３０５４に供給される。従って、ＳＡＭ３０５１～３０５４において、権利書データ１０６に基づいて、コンテンツプロバイダ３０１の意向通りに、コンテンツファイルＣＦの利用を行わせることができる。すなわち、ＥＭＤシステム３００によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織７２５に頼ることなく、技術的な手段によって、コンテンツプロバイダ３０１の所有者の権利および利益を確実に守ることができる。

【０４２２】以下、上述した第２実施形態のＥＭＤシステム３００で採用するセキュアコンテナなどの配送プロトコルについて説明する。図１０８に示すように、コンテンツプロバイダ３０１において作成されたセキュアコンテナ１０４は、インターネット（ＴＣＰ／ＩＰ）あるいは専用線（ＡＴＭ　Ｃｅｌｌ）などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ３１０に提供される。また、サービスプロバイダ３１０は、セキュアコンテナ１０４を用いて作成したセキュアコンテナ３０４を、デジタル放送（ＭＰＥＧ－ＴＳ上のＸＭＬ／ＳＭＩＬ）、インターネット（ＴＣＰ／ＩＰ上のＸＭＬ／ＳＭＩＬ）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク３０３に配給する。また、ユーザホームネットワーク３０３，３０３ｎ内、あるいはユーザホームネットワーク３０２と３０３ｎとの間において、ＳＭＡ相互間で、セキュアコンテナが、家庭内ＥＣ（Electric Commerce）／配信サービス（１３９４シリアルバス・インターフェイス上のＸＭＬ／ＳＭＩＬ）や記録媒体などを用いて転送される。

【０４２３】本発明は上述した実施形態には限定されない。例えば、上述した実施形態では、ＥＭＤサービスセンタ１０２，３０２において、キーファイルＫＦを作成する場合を例示したが、コンテンツプロバイダ１０１，３０１においてキーファイルＫＦを作成してもよい。

【０４２４】

【発明の効果】以上説明したように、本発明のデータ処理装置によれば、コンテンツデータの取り扱いを示す権利書データに基づいてコンテンツデータの購入形態等を決定できる。その結果、権利書データをコンテンツデータの提供に係わる者が作成すれば、コンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図１】図１は、本発明の第１実施形態のＥＭＤシステムの全体構成図である。

【図２】図２は、本発明のセキュアコンテナの概念を説

明するための図である。

【図３】図３は、図１に示すコンテンツプロバイダからＳＡＭに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図４】図４は、図３に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図５】図５は、図３に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図６】図６は、図１に示すコンテンツプロバイダとＥＭＤサービスセンタとの間で行われる登録およびキーファイルの転送を説明するための図である。

【図７】図７は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図８】図８は、コンテンツＩＤを説明するための図である。

【図９】図９は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図１０】図１０は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図１１】図１１は、本実施形態で用いられるＲＯＭ型の記録媒体の第１の例を説明するための図である。

【図１２】図１２は、本実施形態で用いられるＲＯＭ型の記録媒体の第２の例を説明するための図である。

【図１３】図１３は、本実施形態で用いられるＲＯＭ型の記録媒体の第３の例を説明するための図である。

【図１４】図１４は、本実施形態で用いられるＲＡＭ型の記録媒体の第１の例を説明するための図である。

【図１５】図１５は、本実施形態で用いられるＲＡＭ型の記録媒体の第２の例を説明するための図である。

【図１６】図１６は、本実施形態で用いられるＲＡＭ型の記録媒体の第３の例を説明するための図である。

【図１７】図１７は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図１８】図１８は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図１９】図１９は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図２０】図２０は、図１に示すＥＭＤサービスセンタの機能を示す図である。

【図２１】図２１は、図１に示す利用履歴データを説明するための図である。

【図２２】図２２は、図１に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図２３】図２３は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図２４】図２４は、図２２に示す外部メモリに記憶されるデータを説明するための図である。

【図２５】図２５は、作業用メモリに記憶されるデータを説明するための図である。

【図２６】図２６は、図１に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図２７】図２７は、図２３に示す記憶部に記憶されるデータを説明するための図である。

【図２８】図２８は、ＥＭＤサービスセンタからライセンス鍵データを受信する際のＳＡＭの処理を示すフローチャートである。

【図２９】図２９は、セキュアコンテナを入力する際のＳＡＭの処理を示すフローチャートである。

【図３０】図３０は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図３１】図３１は、コンテンツデータの購入形態を決定する際のＳＡＭの処理を示すフローチャートである。

【図３２】図３２は、購入形態が決定されたセキュアコンテナを説明するための図である。

【図３３】図３３は、コンテンツデータを再生する際のＳＡＭの処理を示すフローチャートである。

【図３４】図３４は、図２２に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送し、ＡＶ機器において再購入を行う場合を説明するための図である。

【図３５】図３５は、図３４に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図３６】図３６は、図３４に示す処理を示すフローチャートである。

【図３７】図３７は、図３４において転送されるセキュアコンテナのフォーマットを説明するための図である。

【図３８】図３８は、図３４に示す場合において、転送先のＳＡＭにおいて、入力したコンテンツファイルなどを、ＲＡＭ型あるいはＲＯＭ型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図３９】図３９は、図３４に示す場合における転送先のＳＡＭの処理を示すフローチャートである。

【図４０】図４０は、図３４に示す場合における転送先のＳＡＭの処理を示すフローチャートである。

【図４１】図４１は、図１に示すユーザホームネットワーク内のＳＡＭにおける各種の購入形態を説明するための図である。

【図４２】図４２は、コンテンツの購入形態が未決定の図１１に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する場合を説明するための図である。

【図４３】図４３は、図４２に示す場合におけるＡＶ機器のＳＡＭ内でのデータの流れを示す図である。

【図４４】図４４は、図４２に示す場合におけるＳＡＭの処理のフローチャートである。

【図４５】図４５は、ユーザホームネットワーク内のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して、これを他のＡＶ機器に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図４６】図４６は、図４５に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図４７】図４７は、図４５において、転送元のＳＡＭから転送先のＳＡＭに転送されるセキュアコンテナのフォーマットを説明するための図である。

【図４８】図４８は、図４５の場合における、転送元および転送先のＳＡＭの処理のフローチャートを示す図である。

【図４９】図４９は、図４５の場合における、転送元および転送先のＳＡＭの処理のフローチャートを示す図である。

【図５０】図５０は、図４５に示す場合における転送先のＳＡＭ内でのデータの流れを示す図である。

【図５１】図５１は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図５２】図５２は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図５３】図５３は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図５４】図５４は、ＳＡＭが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図５５】図５５は、ＥＭＤサービスセンタが作成する公開鍵証明書破棄リストのフォーマットを説明するための図である。

【図５６】図５６は、ＥＭＤサービスセンタが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図５７】図５７は、ＳＡＭが持つセキュリティ機能を説明するための図である。

【図５８】図５８は、コンテンツプロバイダからネットワーク機器に送信されたセキュアコンテナに格納されたコンテンツデータをＡＶ機器（ストレージ機器）において記録媒体（メディア）に書き込む際に行われる、コンテンツプロバイダ、ＳＡＭ相互間のセキュリティ機能を説明するための図である。

【図５９】図５９（Ａ）は一般的に用いられるＯＳＩ参照モデルにおける送信側および受信側の各層（レイヤー）で行われる通信を説明するための図、図５９（Ｂ）は図５８に示すコンテンツプロバイダとネットワーク機器（ＳＡＭ）との間での通信時の保護機能を詳細に説明するための図である。

【図６０】図６０は、図５８に示すネットワーク機器（ＳＡＭ）とＡＶ機器（ＳＡＭ）との間の通信時の保護機能を詳細に説明するための図である。

【図６１】図６１は、例えば、図１に示すーのＡＶ機器において図１１に示すＲＯＭ型の記録媒体からコンテンツデータを再生し、当該再生したコンテンツデータをバスを介して他のＡＶ機器に伝送し、当該他のＡＶ機器において図１４に示すＲＡＭ型の記録媒体に記録する場合のセキュリティ処理を説明するための図である。

【図６２】図６２は、図１に示すユーザホームネットワーク内の例えばネットワーク機器内での各種のＳＡＭに搭載形態の一例を説明するための図である。

【図６３】図６３は、権利処理用のＳＡＭの回路モジュールの第１形態を説明するための図である。

【図６４】図６４は、図６３に示す回路モジュールを用いた場合のＳＡＭ内のハードウェア構成の一例を説明するための図である。

【図６５】図６５は、権利処理用のＳＡＭの回路モジュールの第２形態を説明するための図である。

【図６６】図６６は、メディアＳＡＭの回路モジュールの第１形態を説明するための図である。

【図６７】図６７は、ＲＯＭ型の記録媒体のメディアＳＡＭの出荷時における記憶データを説明するための図である。

【図６８】図６８は、ＲＯＭ型の記録媒体のメディアＳＡＭの登録後における記憶データを説明するための図である。

【図６９】図６９は、ＲＡＭ型の記録媒体のメディアＳＡＭの出荷時における記憶データを説明するための図である。

【図７０】図７０は、ＲＡＭ型の記録媒体のメディアＳＡＭの登録後における記憶データを説明するための図である。

【図７１】図７１は、メディアＳＡＭの回路モジュールの第２形態を説明するための図である。

【図７２】図７２は、メディアＳＡＭの回路モジュールの第３形態を説明するための図である。

【図７３】図７３は、メディアＳＡＭの回路モジュールの第４形態を説明するための図である。

【図７４】図７４は、メディアＳＡＭの回路モジュールの第５形態を説明するための図である。

【図７５】図７５は、メディアＳＡＭの回路モジュールの第６形態を説明するための図である。

【図７６】図７６は、メディアＳＡＭの回路モジュールの第７形態を説明するための図である。

【図７７】図７７は、ＡＶ圧縮・伸長用ＳＡＭの回路モジュールの第１形態を説明するための図である。

【図７８】図７８は、ＡＶ圧縮・伸長用ＳＡＭの回路モジュールの第２形態を説明するための図である。

【図７９】図７９は、メディア・ドライブＳＡＭの回路モジュールの第１形態を説明するための図である。

【図８０】図８０は、メディア・ドライブＳＡＭの回路モジュールの第２形態を説明するための図である。

【図８１】図８１は、メディア・ドライブＳＡＭの回路モジュールの第３形態を説明するための図である。

【図８２】図８２は、メディア・ドライブＳＡＭの回路モジュールの第４形態を説明するための図である。

【図８３】図８３は、図１に示すＥＭＤシステムの全体動作のフローチャートである。

【図８４】図８４は、第１実施形態のＥＭＤシステムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図８５】図８５は、本発明の第２実施形態のＥＭＤシステムの全体構成図である。

【図８６】図８６は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図８７】図８７は、図８５に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図８８】図８８は、図８７に示すセキュアコンテナに格納されたコンテンツファイルの送信形態を説明するための図である。

【図８９】図８９は、図８７に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図９０】図９０は、図８５に示すＥＭＤサービスセンタの機能を示す図である。

【図９１】図９１は、図８５に示すネットワーク機器の構成図である。

【図９２】図９２は、図９１に示すＣＡモジュールの機能ブロック図である。

【図９３】図９３は、図８５に示すＳＡＭの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図９４】図９４は、図９３に示す作業用メモリに記憶されるデータを説明するための図である。

【図９５】図９５は、図８５に示すＳＡＭの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図９６】図９６は、図８５に示すＳＡＭにおけるセキュアコンテナの入力処理の手順を示すフローチャートである。

【図９７】図９７は、図８５に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合を説明するための図である。

【図９８】図９８は、図８５に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送先のＳＡＭ内での処理の流れを説明するための図である。

【図９９】図９９は、図９８に示す転送元のＳＡＭの処理を示すフローチャートである。

【図１００】図１００は、図９７に示す場合に、転送元のＳＡＭから転送先のＳＡＭに転送されるセキュアコンテナのフォーマットを示す図である。

【図１０１】図１０１は、図９７に示す場合の転送先のＳＡＭ内でのデータの流れを示す図である。

【図１０２】図１０２は、図９７に示す場合の転送先のＳＡＭの処理のフローチャートである。

【図１０３】図１０３は、図９７に示す場合の転送先のＳＡＭの処理のフローチャートである。

【図１０４】図１０４は、図８５に示すユーザホームネットワーク内でのＳＡＭの接続形態の一例を説明するための図である。

【図１０５】図１０５は、図８５に示すＥＭＤシステムの全体動作のフローチャートである。

【図１０６】図１０６は、図８５に示すＥＭＤシステムの全体動作のフローチャートである。

【図１０７】図１０７は、図８５に示すＥＭＤシステムのサービス形態の一例を示す図である。

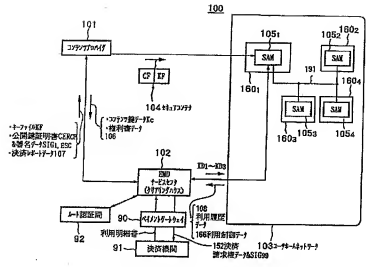
【図１０８】図１０８は、図８５に示すＥＭＤシステムにおいて採用されるセキュアコンテナの配送プロトコルを説明するための図である。

【図１０９】図１０９は、従来のＥＭＤシステムの構成図である。

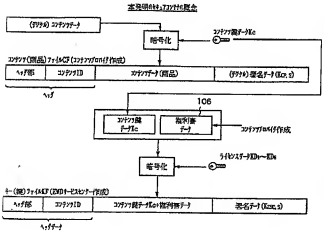
【符号の説明】

９０…ペイメントゲートウェイ，９１…決済機関，９２…ルート認証局，１００，３００…ＥＭＤシステム，１０１，３０１…コンテンツプロバイダ，１０２，３０２…ＥＭＤサービスセンタ，１０３，３０３…ユーザホームネットワーク，１０４，３０４…セキュアコンテナ，105_1～105_4，305_1～305_4…ＳＡＭ，１０６…権利書データ，１０７，３０７…決済レポートデータ，１０８，３０８…利用履歴データ，160_1…ネットワーク機器，160_2～160_4…ＡＶ機器，１５２，１５２ｃ，１５２ｓ…決済指示データ，１９１…バス，３１０…サービスプロバイダ，３１１…ＣＡモジュール，３１２…プライスタグデータ，ＣＦ…コンテンツファイル，ＫＦ…キーファイル，Ｋｃ…コンテンツ鍵データ

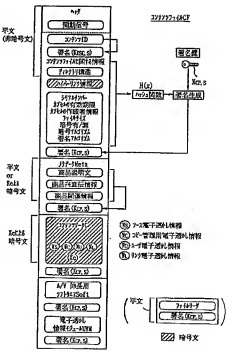
【図１】


100
101
コンテンツプロバイダ
CP EP
104 セッションコンテンツ
・コンテンツ鍵データKc
・権利情報データ
106
・ユーザ公開鍵証明書CERTU
・署名データSIGTU, ESC
・決済レポートデータ107
102
DVD
ナビセンタ
(ライセンスプロバイダ)
KD1～KD3
105₁
105₂
160₂
SAM
191
160₄
160₁
SAM
SAM
160₃
105₃
105₄
ルート認証局
90
ペイメントゲートウェイ
108
利用履歴
データ
166利用制御データ
利用明細書
92
91
決済機関
163ユーザ・メッセージ
決済指示データ&SIGU

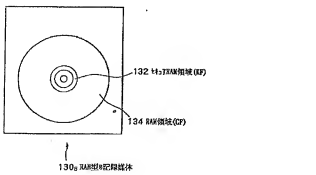
【図２】


本発明data, フォルダ構造
(データ) コンテンツデータ
暗号化
コンテンツ鍵データKc
コンテンツ(商品) フォルダCF (コンテンツプロバイダ作成)
ヘッダ部
コンテンツID
コンテンツデータ(商品)
(データ)署名データ(Kcr, s)
ヘッダ
106
コンテンツ鍵データKc
権利情報データ
コンテンツプロバイダ作成
暗号化
ライセンスキーKD1～KDn
ナビ(端末)フォルダEP (DVDナビセンター作成)
ヘッダ部
コンテンツID
コンテンツ鍵データKc+権利情報データ
署名データ(Kcnt, s)
ヘッダデータ

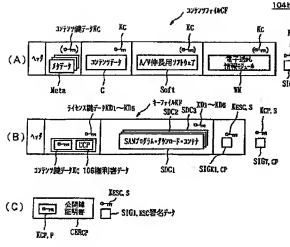
【図４】


ヘッダ
コンテンツプロバイダCP
平文
(非暗号文)
暗号鍵
コンテンツID
署名 (Kcnr, s)
フォルダ1の利用許可情報
アイコン情報
コンテンツ属性情報
コンテンツキー
カテゴリ1の暗号鍵
カテゴリ2の暗号鍵
カテゴリ3の暗号鍵
署名 (Kcr, s)
電子透かし
H(x)
ハッシュ関数
署名作成
署名鍵
Kcr, s
ノンリターンMenu
商品説明情報
販売実績情報
著作権情報
署名 (Kcr, s)
平文
or
Kcl1
暗号文
Kc2,3
暗号文
1
2
3
4
5
署名 (Kcr, s)
A/V 記録用
フォルダ(Dvd1)
署名 (Kcr, s)
電子透かし
検証データ
署名 (Kcr, s)
① ユーザ電子透かし情報
② コピー管理用電子透かし情報
③ レート電子透かし情報
④ ロット電子透かし情報
平文
フォルダ
署名 (Kcr, s)
暗号文

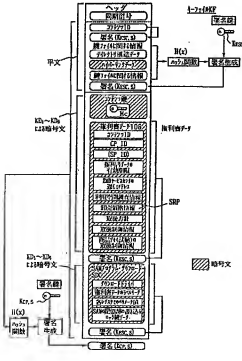
【図１６】


132 セクタIDAM領域 (IDF)
134 RAM領域(DF)
130₀ RAM型光記録媒体

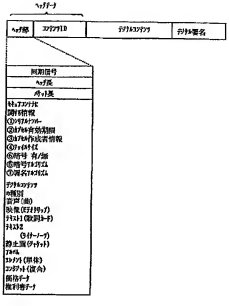
【図３】



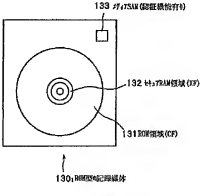
【図５】



【図７】



【図１１】

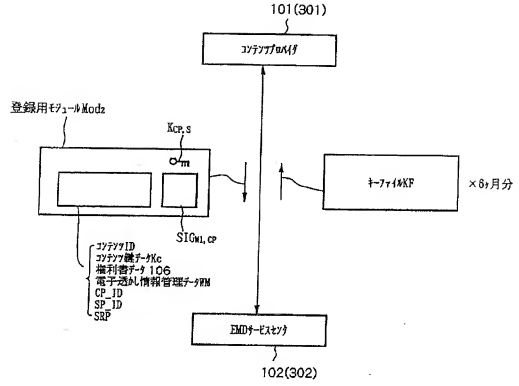


【図２４】

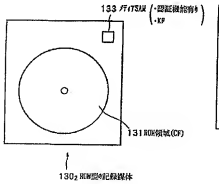
外部利用装置201に記憶されるデータ

利用装置データ108
SAM 管理切り
(ICPデータのロードだけにデータ SAM が用いられる)

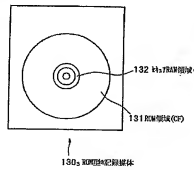
【図６】



【図１２】



【図１３】



【図２５】

作業用メモリ320に記憶されるデータ

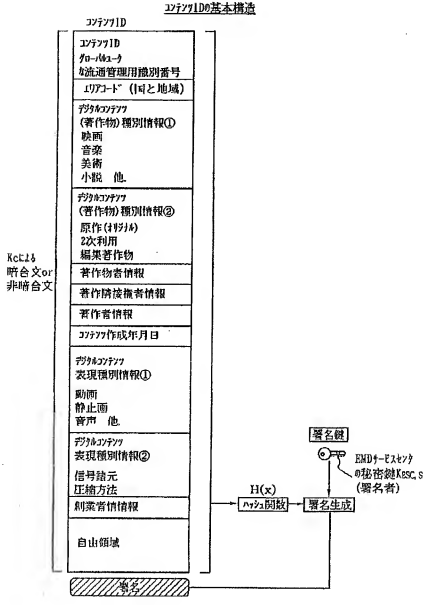
コンテンツ鍵データKc
権利書データ(UCP)106
相互認証(チャレンジ&レスポンス)で使用するセッション鍵データKm
コンテンツプロバイダ101の公開鍵証明書CERp
利用制御データ(UCS)166
SAMアダプタ4・ダウンロード・コマンドSD₁～SDCn

【図９４】

作業用メモリ320に記憶されるデータ

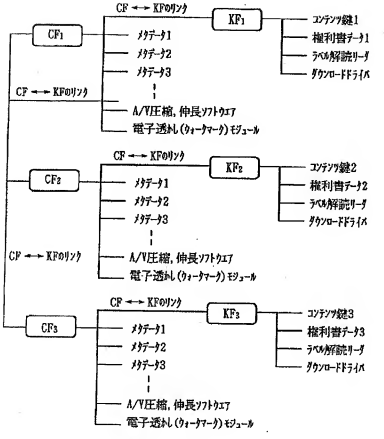
コンテンツ鍵データKc
権利書データ(UCP)106
ポイント残高データPD106のセッション鍵データKm
コンテンツプロバイダ101の公開鍵証明書データCERp
サービスプロバイダ301の公開鍵証明書データCERm
利用制御データ(UCS)166
SAMアダプタ4・ダウンロード・コマンドSD₁～SDCn
プライスデータP312

【図８】


コンテンツIDの基本構造
コンテンツID
コンテンツID
グローバルユニークな流通管理用識別番号
エリアコード（国と地域）
デジタルコンテンツ（著作物）種別情報①
映画
音楽
美術
小説　他
デジタルコンテンツ（著作物）種別情報②
原作（オリジナル）
2次利用
編集著作物
著作物者情報
著作隣接権者情報
著作者情報
コンテンツ作成年月日
デジタルコンテンツ表現種別情報①
動画
静止画
音声　他
デジタルコンテンツ表現種別情報②
信号諸元
圧縮方法
創業者情報
自由領域
署名
Kcによる暗号文or非暗号文
署名鍵
ENDキーEスセンタの秘密鍵Kesc.s（署名者）
H(x)
ハッシュ関数
署名生成

【図９】

セキュアコンテンツのディレクトリ構造

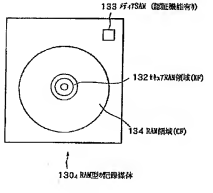


【図２１】

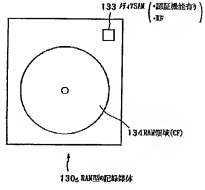
利用履歴データ108(308)

ESC_コンテンツID
CP_コンテンツID
(SP_コンテンツID)
ユーザID
ユーザ情報
SAM_ID
HNG_ID
ディスカウント情報
トレーシング情報
(プライスタグデータPT)
CP_ID
(SP_ID)
紹介業者(ポータル:Portal)ID
ハードウェア提供者ID
Media_ID
コンポーネントID
ライセンス所有者の識別子LH_ID
ESC_ID

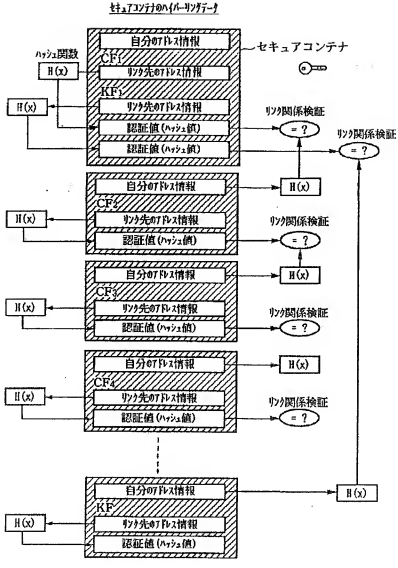
【図１４】



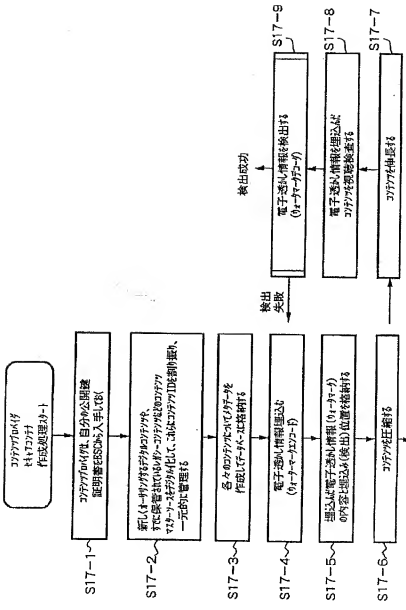
【図１５】



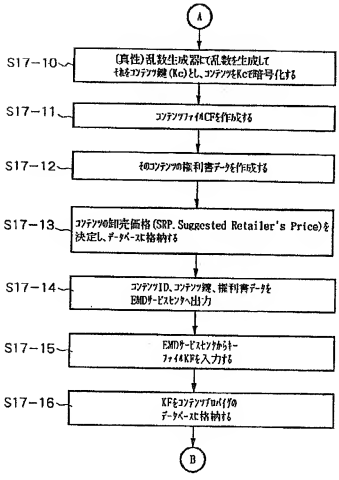
【図１０】


セキュアコンテナのハイパーリンクデータ
ハッシュ関数
H(x)
自分のアドレス情報
CF1
リンク先のアドレス情報
KF1
リンク先のアドレス情報
認証値(ハッシュ値)
認証値(ハッシュ値)
セキュアコンテナ
リンク関係検証
= ?
リンク関係検証
= ?
自分のアドレス情報
CF2
リンク先のアドレス情報
認証値(ハッシュ値)
H(x)
リンク関係検証
= ?
自分のアドレス情報
CF3
リンク先のアドレス情報
認証値(ハッシュ値)
H(x)
リンク関係検証
= ?
自分のアドレス情報
CF4
リンク先のアドレス情報
認証値(ハッシュ値)
H(x)
リンク関係検証
= ?
自分のアドレス情報
KF
リンク先のアドレス情報
認証値(ハッシュ値)
H(x)
H(x)

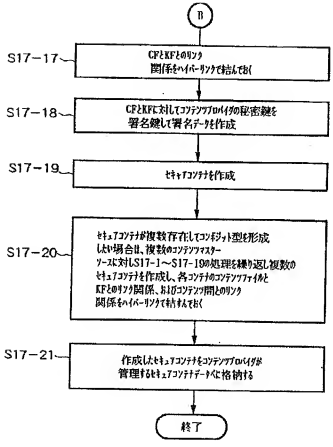
【図１７】


コンテンツのIDや
それぞれの
作成処理者など
S17－1
コンテンツのIDや、自分が公開設
定時点でSSDに入手した旨
S17－2
新しくオリジナルデジタルコンテンツや、
すでに保管されているオリジナル記録コンテンツ
マスターコンテンツなどを記録して、これらコンテンツのID生成時点を含め、
一元的に管理する
S17－3
各々のコンテンツについてハッシュ値を
作成しインデックス・ID情報付与
S17－4
電子透かし情報埋込み
（ウォーターマーク２－１）
S17－5
埋込み電子透かし情報（ウォーター
マーク２－１）の内容と埋込み（検出）位置を情報付与
S17－6
コンテンツ圧縮する
A
検出
失敗
検出成功
S17－9
電子透かし情報を検出する
（ウォーターマーク２）
S17－8
電子透かし情報と埋込み
コンテンツを照合検査する
S17－7
コンテンツを伸長する

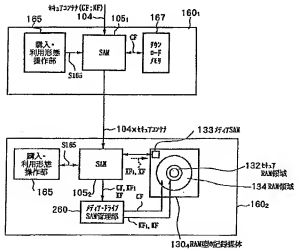
【図１８】


A
S17−10
(真性)乱数生成器にて乱数を生成して
それをコンテンツ鍵(Kc)とし、コンテンツをKcで暗号化する
S17−11
コンテンツファイルCFを作成する
S17−12
そのコンテンツの権利書データを作成する
S17−13
コンテンツの卸売価格(SRP、Suggested Retailer's Price)を
決定し、データベースに格納する
S17−14
コンテンツID、コンテンツ鍵、権利書データを
EMDサービスセンタへ出力
S17−15
EMDサービスセンタからキー
ファイルKFを入力する
S17−16
KFをコンテンツプロバイダの
データベースに格納する
B

【図１９】


B
S17－17
CFとKFとのリンク
関係をハイパーリンクで結んでおく
S17－18
CFとKFに対してコンテンツプロバイダの秘密鍵を
署名鍵として署名データを作成
S17－19
セキュアコンテナを作成
S17－20
セキュアコンテナが複数存在してコンポジット型を形成
しない場合は、複数のコンテンツマスター
ソースに対しS17－1～S17－19の処理を繰り返し、複数の
セキュアコンテナを作成し、各コンテナのコンテンツファイルと
KFとのリンク関係、およびコンテンツ間とのリンク
関係をハイパーリンクで結んでおく
S17－21
作成したセキュアコンテナをコンテンツプロバイダが
管理するセキュアコンテナデータベースに格納する
終了

【図３４】


セキュアコンテナ(CF,KF)
165
104
105₁
167
160₁
購入・利用形態操作部
SAM
CF
ダウンロードプログラム
S16a
104×セキュアコンテナ
133ディスクSAM
S185
購入・利用形態操作部
SAM
KF₁, KF
132セキュアRAM領域
134 RAM領域
CF, KF₁
KF
CF
185
105₂
160₂
260
ディスクドライブSAM管理部
KF₁, KF
130₄RAM領域記録媒体

【図２０】

EMDサービスセンタ102の主な機能

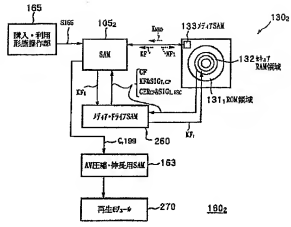
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データCERcp, CERSAM1～CERSAMnの発行

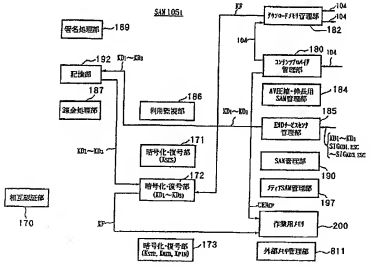
キーファイルKFの生成

利用履歴データに基づいた決済処理(利益分配処理)

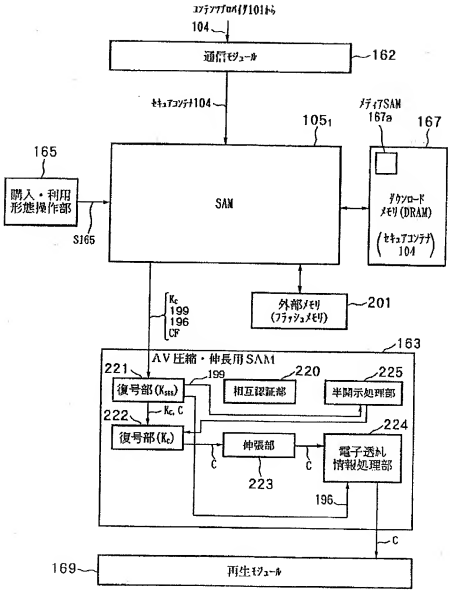
【図４２】



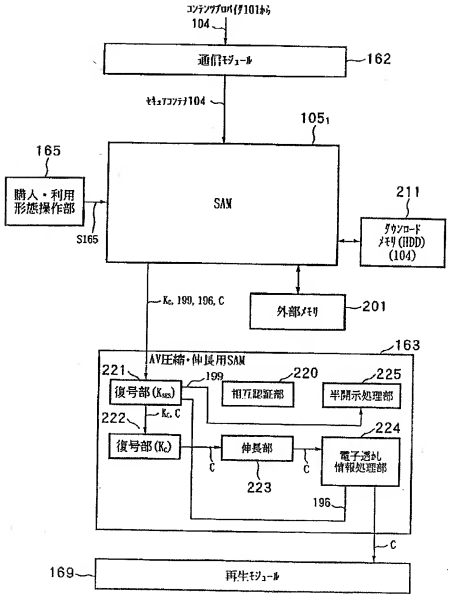
【図２３】



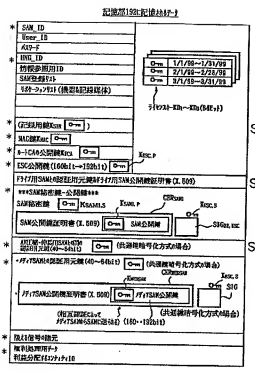
【図２２】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
メディアSAM
167a
167
1051
165
購入・利用
形態操作部
SAM
ダウンロード
メモリ(DRAM)
セキュアコンテナ
104
SJ65
Ke
199
196
CF
外部メモリ
(フラッシュメモリ)
201
163
AV圧縮・伸長用SAM
221
復号部(Kssl)
199
相互認証部
220
半開示処理部
225
222
Ke, C
復号部(Kc)
伸張部
224
電子透かし
情報処理部
C
C
223
196
C
169
再生モジュール

【図２６】

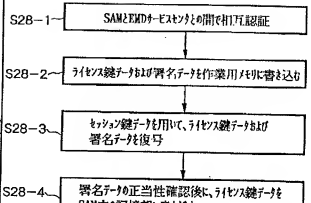

コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
165
購入・利用形態操作部
S165
SAM
211
ダウンロードメモリ(HDD)(104)
Ke, 199, 196, C
外部メモリ
201
163
AV圧縮・伸長用SAM
221
復号部(Kcnt)
199
相互認証部
220
半開示処理部
225
222
Kc, C
復号部(Kc)
伸長部
224
電子透かし情報処理部
C
223
196
C
169
再生モジュール

【図２７】



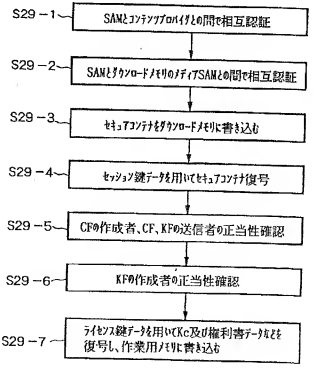
【図２８】

ライセンス鍵データ受信処理(SAM)

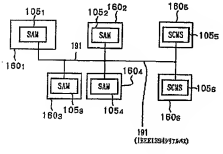


【図２９】

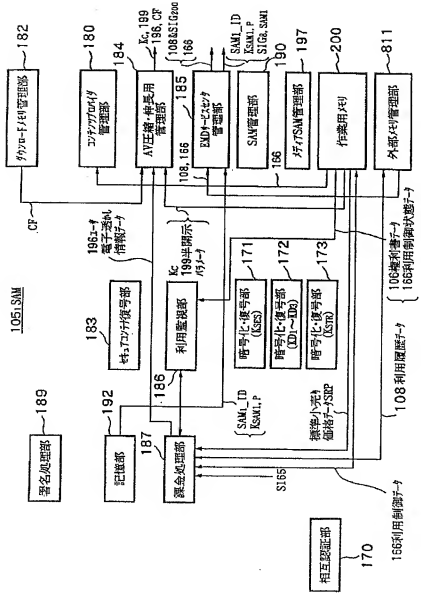
セキュアコンテナの入力処理(SAM)



【図５３】

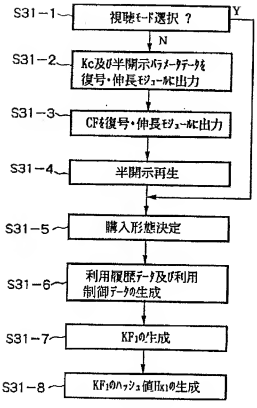


【図３０】

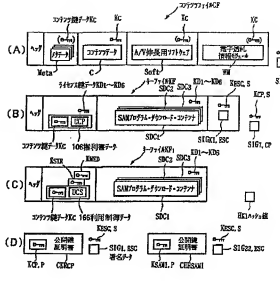

182
ダウンロード許可管理部
CR
180
コンテンツ(DVD)管理部
184
AVC装置・使用管理部
Kc, 199
196, CF
108&SIGpos
166
185
108, 166
DVD-ビデオ管理部
SAM1_ID
KSAM1_P
SIGpos, SAM1
190
SAM管理部
106
197
メディアSAM管理部
200
作業用メモリ
811
外部メモリ管理部
105 SAM
189
署名処理部
192
記憶部
187
課金処理部
183
セキュアな保守部
186
利用監視部
Kc
199 使用制限
パラメータ
195 コンテンツ
暗号化情報データ
SAM1_ID
KSAM1_P
171
暗号化・復号部
(KSAS)
172
暗号化・復号部
(DDI～DDS)
173
暗号化・復号部
(KSTR)
標準小売価格データ SBP
S165
108 利用履歴データ
106 権利書データ
166 利用制御状態データ
166 利用制御データ
170
相互認証部

【図３１】

購入形態決定処理

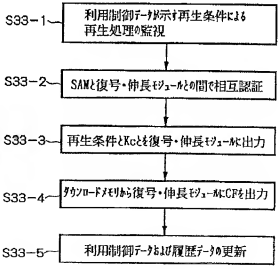


【図３２】

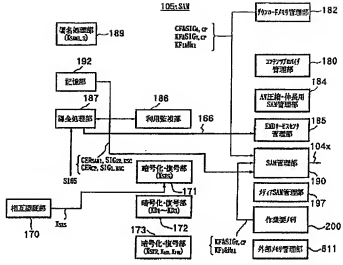


【図３３】

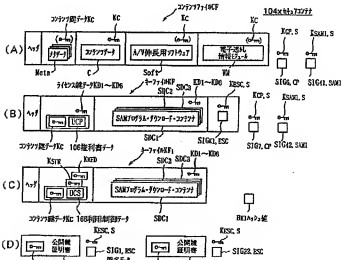
コンテンツデータの再生処理



【図３５】

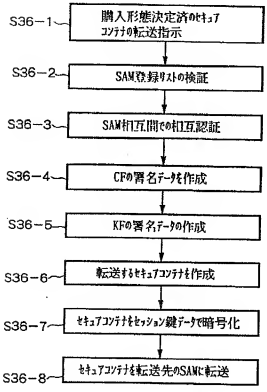

105:SAM
署名処理部 (Sign1,S)
189
CPAS1Gn, CP
KPAS1G, CP
KPAnRn
192
記憶部
187
186
鍵生成部
利用監視部
166
CERn01, S1Gn, ESC
CERn, S1G, ESC
S105
暗号化・復号部 (DES)
171
相互認証部
Rnn
170
暗号化・復号部 (DES—KEn)
173
172
暗号化・復号部 (KEn, Rn, Rn)
KPAS1G, CP
KPAnRn
ﾀｸｼｰF/W管理部
182
ｺﾝﾃﾝﾂDB(F)管理部
180
184
ATC正規・休眠用SAM管理部
ｶｰﾄﾞﾘｰﾀﾞｰﾗｲﾀ管理部
185
104x
SAM管理部
190
ｵﾌﾗｲﾝSAM管理部
197
作業実行部
200
外部ｱﾌﾟﾘ管理部
811

【図３７】


(A)
(B)
(C)
(D)
Meta
Soft
KEn—KDn
SAMﾌﾟﾛﾌﾞﾗﾑ・ﾌﾟﾛｸﾞﾗｰﾄﾞ・ｺﾝﾃﾝﾂ
SBC1
SBC2
SBC3
KSTK
KNEB
S1G1, ESC
S1G2, SAM1
S1G3, CP
S1G4, SAM1
S1G1, CP
S1G2, ESC
S1G23, ESC
CER1, P
CER2, P
KSM1, P
CERSAM1
公開鍵証明書
署名データ

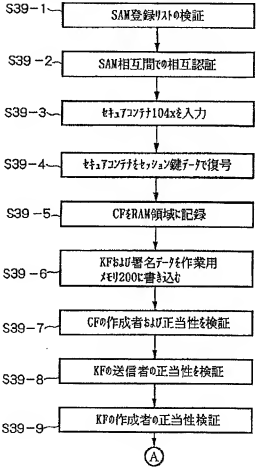
【図３６】

一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送先のSAMの処理

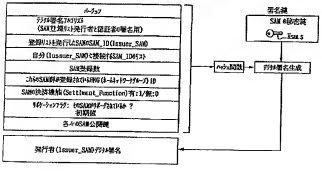


【図３９】

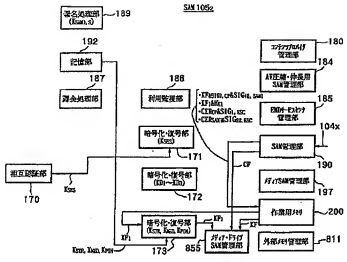
一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送先のSAMの処理



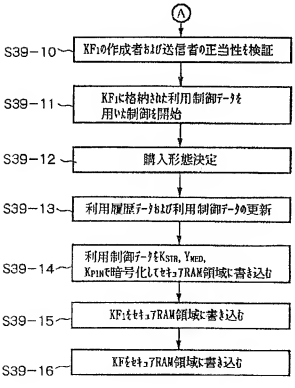
【図５４】



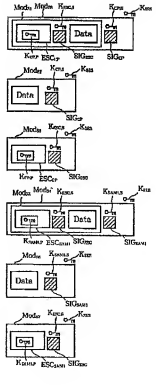
【図３８】


SAM 105x
署名処理部 (Ksam, x)
189
192
記憶部
187
演算処理部
188
利用管理部
KF#STR, CR&STGR, KMD
KF#MD
CERtoSTGR, KEC
CERtoMDSTGR, KEC
コンテンツ/KM/ID 管理部
180
ATE認証・鍵配信 SAM管理部
184
EMD#-EKEY 管理部
185
104x
暗号化・復号部 (KSEC)
171
暗号化・復号部 (KEK→KEK)
172
SAM管理部
190
CF
KF/SAM管理部
197
作業用メモリ
200
外部I/F管理部
811
相互認証部
170
Kmu
暗号化・復号部 (Kmu, Kmu, Kmu)
KF1
173
KF1
855
KF2
Kmu, Kmu, Kmu

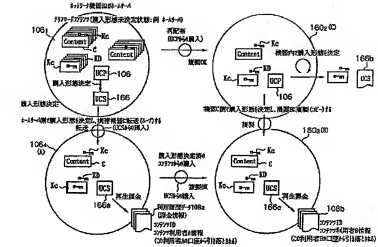
【図４０】


A
S39−10
KF1の作成者および送信者の正当性を検証
S39−11
KF1に格納された利用制御データを用いた制御を開始
S39−12
購入形態決定
S39−13
利用履歴データおよび利用制御データの更新
S39−14
利用制御データをKSTR, VMED, KP1MCで暗号化してセキュアRAM領域に書き込む
S39−15
KF1をセキュアRAM領域に書き込む
S39−16
KFをセキュアRAM領域に書き込む
(A) 101(CP)→SAM105x (ｲﾝﾎﾟｰﾄ)
(B) 101(CP)→SAM105x (ｲﾝﾎﾟｰﾄ)
(C) 102(ESC)→SAM105x (ｲﾝﾎﾟｰﾄ)
(D) SAM105x→101(CP) (ｴｸｽﾎﾟｰﾄ)
(E) SAM105x→101(CP) (ｲﾝﾎﾟｰﾄ)
(F) 102(ESC)→101(CP) (ｲﾝﾎﾟｰﾄ)

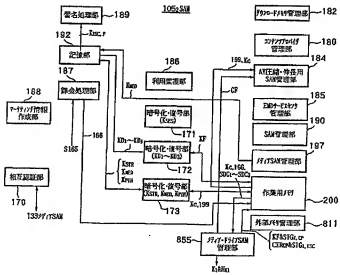
【図５１】


Data
Data
Data
Data
Data

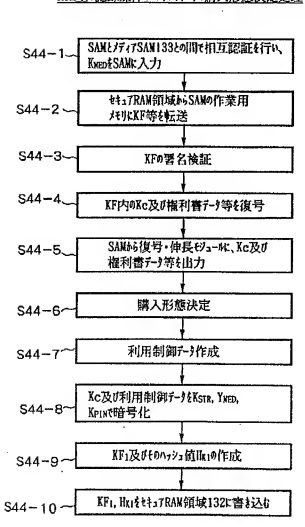
【図４１】



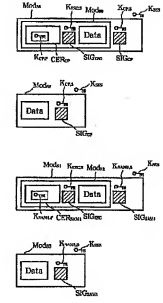
【図４３】



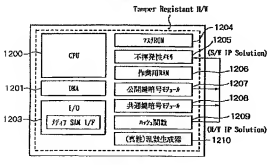
【図４４】



【図５２】

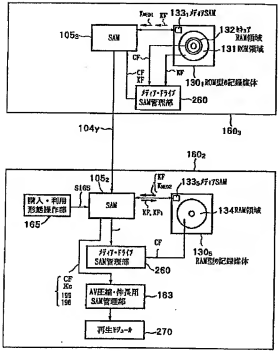


【図６６】

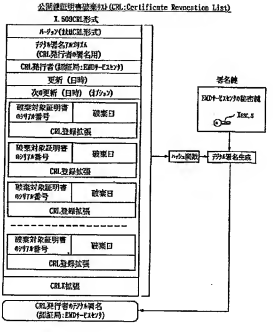


FF1SAM133a

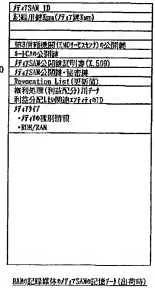
【図４５】



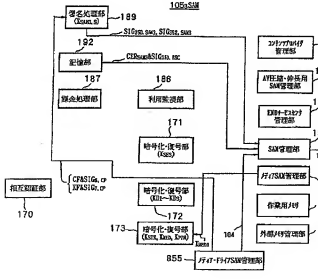
【図５５】



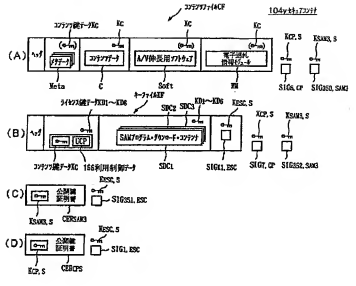
【図６９】



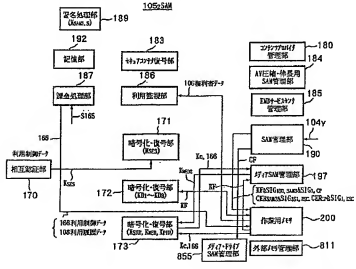
【図４６】



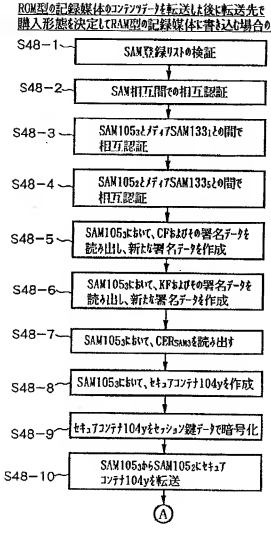
【図４７】



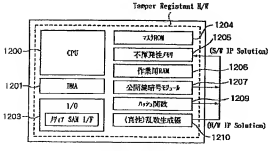
【図５０】



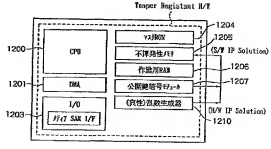
【図４８】


ROM型の記録媒体のコンテンツデータを転送した後に転送先で
購入形態を決定してRAM型の記録媒体に書き込む場合の処理
S48－1
SAM登録リストの検証
S48－2
SAM相互間での相互認証
S48－3
SAM105₂とメディアSAM133₁との間で
相互認証
S48－4
SAM105₂とメディアSAM133₂との間で
相互認証
S48－5
SAM105₂において、CPおよびその署名データを
読み出し、新たな署名データを作成
S48－6
SAM105₂において、KPおよびその署名データを
読み出し、新たな署名データを作成
S48－7
SAM105₂において、CERSAM2を読み出す
S48－8
SAM105₂において、セキュアコンテナ104yを作成
S48－9
セキュアコンテナ104yをセッション鍵データで暗号化
S48－10
SAM105₂からSAM105₁にセキュア
コンテナ104yを転送
A

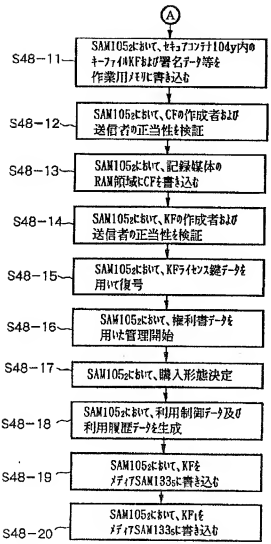
【図７１】


Tamper Registant H/W
1204
1205
(S/W IP Solution)
1206
1207
1209
1210
(S/W IP Solution)
1200
1201
1203
CPU
DMA
I/O
メディアSAM I/F
マスクROM
不揮発性メモリ
作業用RAM
公開鍵暗号セクション
ハッシュ関数
(共有)乱数生成器
メディアSAM133b

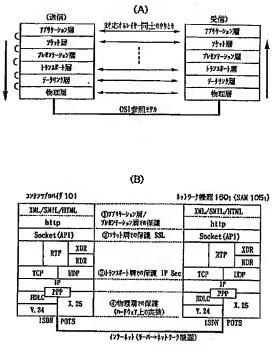
【図７２】


Tamper Registant H/W
1204
1205
(S/W IP Solution)
1206
1207
1210
(S/W IP Solution)
1200
1201
1203
CPU
DMA
I/O
メディアSAM I/F
マスクROM
不揮発性メモリ
作業用RAM
公開鍵暗号セクション
(共有)乱数生成器
メディアSAM133c

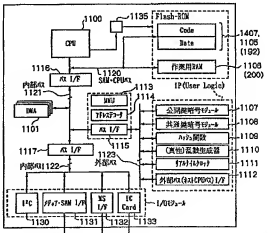
【図４９】



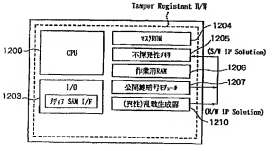
【図５９】



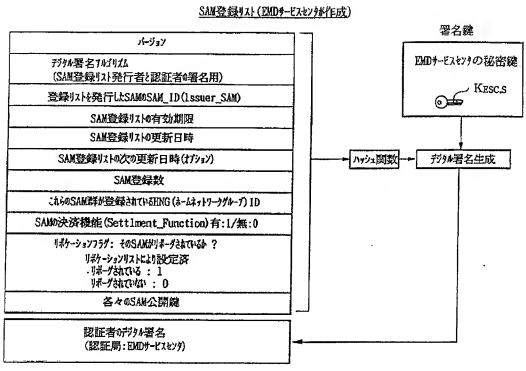
【図６４】



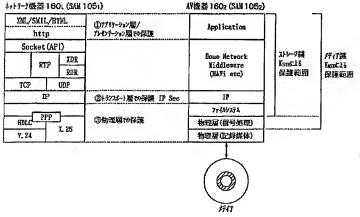
【図７３】



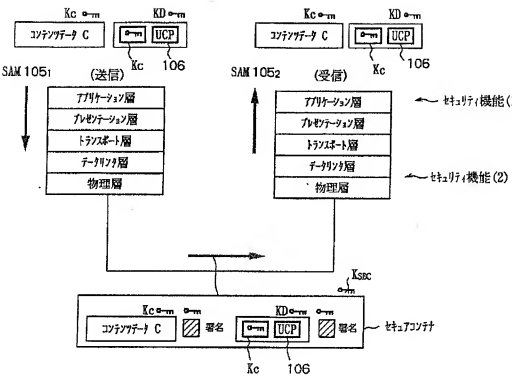
【図５６】


SAM登録リスト(EMDサービスセンタ作成)
署名鍵
EMDサービスセンタの秘密鍵
KESC,S
バージョン
デジタル署名アルゴリズム
(SAM登録リスト発行者と認証者が署名用)
登録リストを発行したSAMのSAM_ID(Issuer_SAM)
SAM登録リストの有効期限
SAM登録リストの更新日時
SAM登録リストの次の更新日時(オプション)
SAM登録数
これらのSAM群が登録されているSHING(ホームネットワークグループ)ID
SAMの決済機能(Settlment_Function)有:1/無:0
リポケーションフラグ: そのSAMがリポートされているか ?
リポケーションリストにより設定済
・リポートされている : 1
リポートされていない : 0
各々のSAM公開鍵
ハッシュ関数
デジタル署名生成
認証者のデジタル署名
(認証局:EMDサービスセンタ)

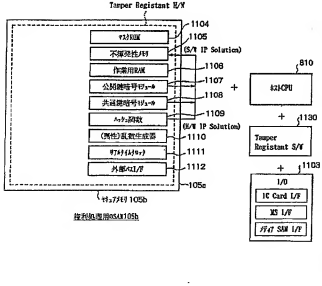
【図６０】


ネットワーク機器 160c (SAM 105c)
AV機器 160a (SAM 105a)
XML/SMIL/HTML
http
①アプリケーション層/
プレゼンテーション層の保護
Application
Socket (API)
RTP
RTCP
UDP
TCP
IP
②トランスポート層での保護 IP Sec
Remote Network Middleware (DLNA etc)
IP
ストリーム鍵 KeyCLS 保護範囲
ファイル鍵 KeyCLS 保護範囲
PPP
HDLC
V.24
V.35
③物理層での保護
ファイルシステム
物理層(信号処理)
物理層(伝送媒体)
メディア

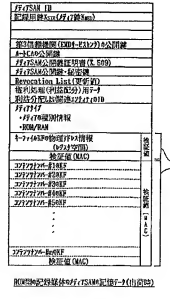
【図５７】


Kc
KD
コンテンツデータ C
UCP
106
SAM 105₁
(送信)
SAM 105₂
(受信)
アプリケーション層
プレゼンテーション層
トランスポート層
データリンク層
物理層
セキュリティ機能(1)
セキュリティ機能(2)
KSBC
署名
セキュアコンテナ

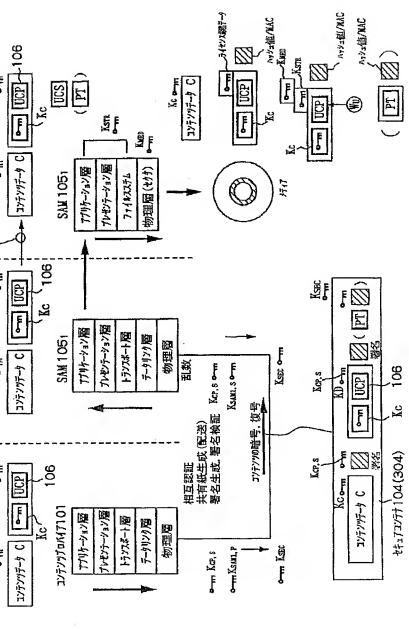
【図６５】


Tamper Registant R/W
1104
1105
(S/W IP Solution)
1106
1107
1108
1109
(S/W IP Solution)
1110
1111
1112
105e
105b
105h
810
1130
1103
I/O
IC Card I/F
XS I/F

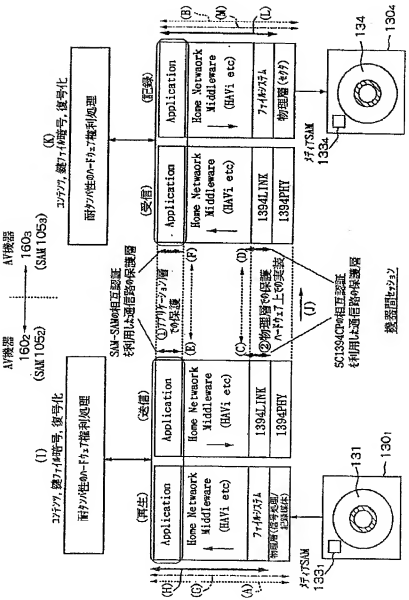
【図６７】


ライセンス鍵KEKによる暗号文

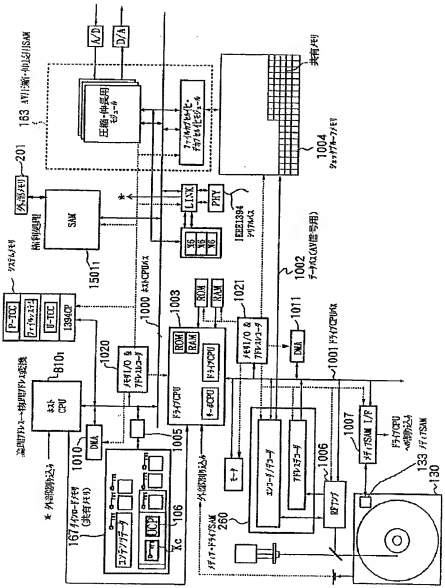
[図５８]


クリアード(購入形態決定)
UCS(Usage Control Status)新規作成
コンテンツデータ C
UCP
106
コンテンツプロバイダ101
アプリケーション層
プレゼンテーション層
トランスポート層
データリンク層
物理層
SAM 105
物理層(セナリ)
乱数
相互認証
非特徴生成(配送)
署名生成・署名検証
コンテンツの暗号、復号
セキュアコンテナ104(304)
PT
UCS
ハウス鍵/MAC
ライト

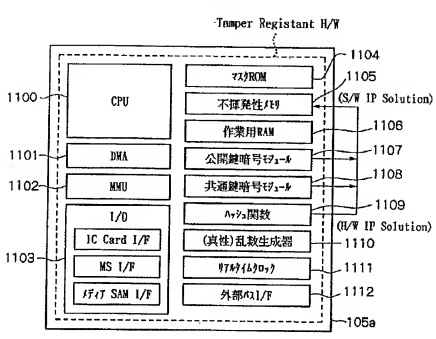
【図６１】


AV機器
160₂
(SAM 105₂)
(I)
コンテンツ，鍵ファイル等，復号化
耐タンパ性のハードウェア権利処理
AV機器
160₃
(SAM 105₃)
(K)
コンテンツ，鍵ファイル等，復号化
耐タンパ性のハードウェア権利処理
SAM-SAM相互認証
&利用以上暗号鍵の保護層
(再生)
(送信)
(受信)
(記録)
Application
Home Network Middleware (HAVi etc)
ファイルシステム
物理層(セクタ)
1394LINK
1394PHY
(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)
(J)
(L)
(M)
(N)
①アプリケーション層
での保護
②物理層での保護
ハードウェア上での保護
SC1394CP相互認証
&利用以上暗号鍵の保護層
機器間セッション
ダイアSAM
133₁
131
130₁
ダイアSAM
133₂
134
130₄

【図６２】



【図６３】

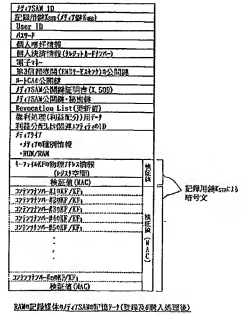


権利処理用のSAM105a

【図６８】

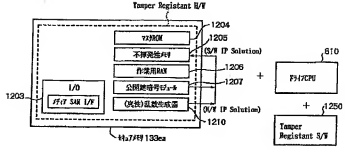
ROM面の記録媒体のメディアSAMの記憶データ(改竄及び購入処理後)

【図７０】

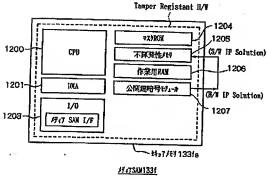


RAM面の記録媒体のメディアSAMの記憶データ(登録及び購入処理後)

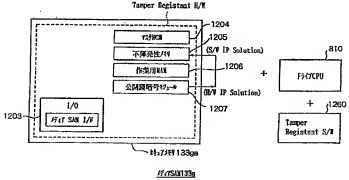
【図７４】


Tamper Registant H/W
1204
ｲﾝｽﾄﾗｸｼｮﾝROM
1205
(S/W IP Solution)
不揮発性ﾒﾓﾘ
作業用RAM
1206
公開鍵暗号ﾌﾟﾛｾｯｻ
1207
(S/W IP Solution)
(光拡散)乱数生成器
1210
1203
I/O
ﾌｨｰﾙﾄﾞ SAN I/F
ﾎｽﾄ7ｲﾝﾁ133ca
ﾌｨｰﾙﾄﾞSAN133a
810
ﾎｽﾄCPU
1250
Tamper Registant S/W

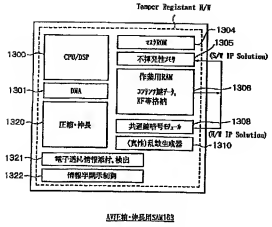
【図７５】


Tamper Registant H/W
1204
ｲﾝｽﾄﾗｸｼｮﾝROM
1205
1200
CPU
不揮発性ﾒﾓﾘ
(S/W IP Solution)
作業用RAM
1206
1201
DMA
公開鍵暗号ﾌﾟﾛｾｯｻ
(S/W IP Solution)
1207
I/O
1208
ﾌｨｰﾙﾄﾞ SAN I/F
ﾎｽﾄ7ｲﾝﾁ133fa
ﾌｨｰﾙﾄﾞSAN133f

【図７６】

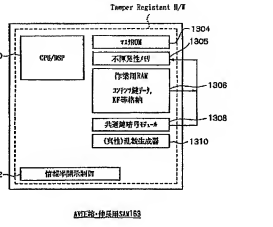

Tamper Registant H/W
1204
ｲﾝｽﾄﾗｸｼｮﾝROM
1205
(S/W IP Solution)
不揮発性ﾒﾓﾘ
1206
作業用RAM
公開鍵暗号ﾌﾟﾛｾｯｻ
(S/W IP Solution)
1207
1203
I/O
ﾌｨｰﾙﾄﾞ SAN I/F
ﾎｽﾄ7ｲﾝﾁ133ga
ﾌｨｰﾙﾄﾞSAN133g
810
ﾎｽﾄCPU
1260
Tamper Registant S/W

【図７７】



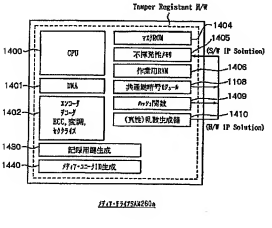
ASIC組・仲具用SAW1段

【図７８】



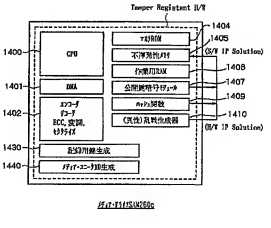
ASIC組・仲具用SAW1段

【図７９】



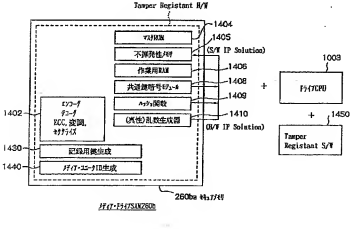
ディスク1セクタ256bit

【図８０】



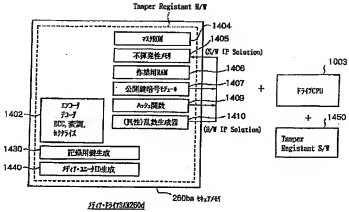
ディスク1セクタ512bit

【図８１】

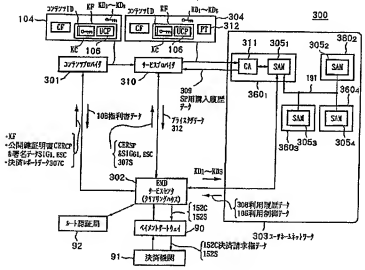


ディスク1セクタ256bit

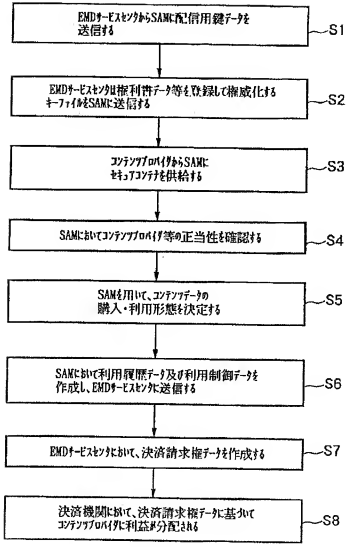
【図８２】


Tamper Registant H/W
1404
1405
(S/W IP Solution)
1406
1407
1409
1410
(S/W IP Solution)
1003
ドライブCPU
1450
Tamper Registant S/W
1402
1430
1440
260bs
260d

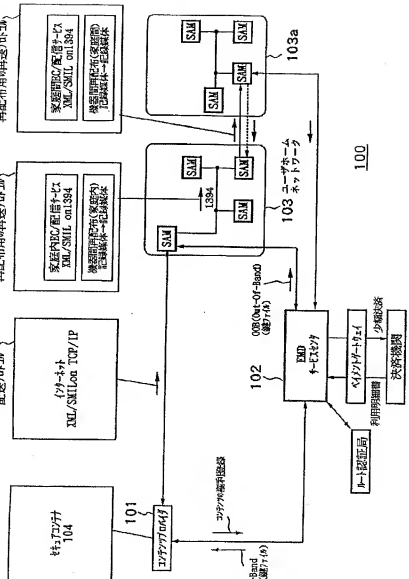
【図８５】


300
104
301
310
106
304
312
3601
3602
3603
3604
3605
191
302
92
91
90
1526
1525
1523

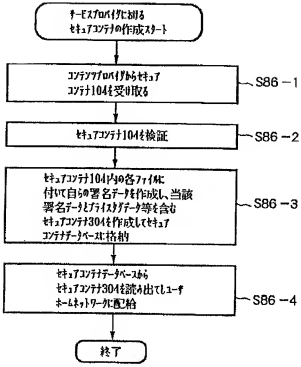
【図８３】


EMDサービスセンタからSAMに配信用鍵データを送信する
S1
EMDサービスセンタは権利情データ等を登録して権威化するキーファイルをSAMに送信する
S2
コンテンツプロバイダからSAMにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダ等の正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データ及び利用制御データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基いてコンテンツプロバイダに利益が分配される
S8

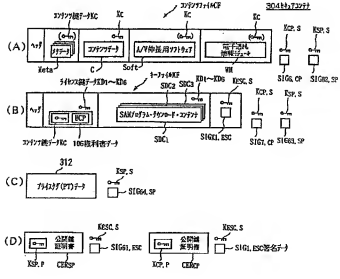
【図８４】


家庭内BD/機器間
再配布用ﾛｰﾐﾝｸﾞﾌｧｲﾙ
家庭内BD/配信ｻｰﾋﾞｽ
XML/SMIL on1394
機器間用記憶(家庭内)
記録媒体→記録媒体
コンテンツDL付用
配信ﾛｰﾐﾝｸﾞﾌｧｲﾙ
ｲﾝﾀｰﾈｯﾄ
XML/SMIL on TCP/IP
ｾｷｭﾘﾃｨﾓｼﾞｭｰﾙ
104
101
コンテンツDL付ｸﾗｲｱﾝﾄ
In-Band
ｷｬﾘｱ(例ｴｱﾛｰﾝ)
ｺﾝﾃﾝﾂ配信認証
102
OOB(Out-of-Band
例ｴｱﾛｰﾝ)
END
ﾉｰﾄﾞｴﾝﾄﾘｰﾎﾟｲﾝﾄ
ﾙｰﾄ認証局
ﾍﾟｲﾒﾝﾄｹﾞｰﾄｳｪｲ
ｼｽﾃﾑ
利用許諾書
決済機関
SAM
1394
103
ﾕｰｻﾞﾎｰﾑ
ﾈｯﾄﾜｰｸ
103a
100

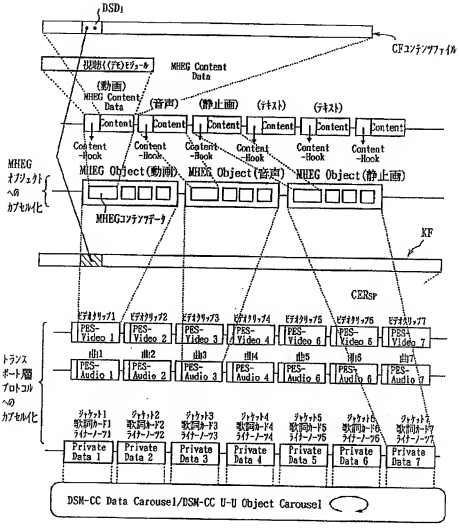
【図８６】


オーサスプロバイダに対する
セキュアコンテナの作成スタート
コンテンツプロバイダからセキュア
コンテナ104を受け取る
S86－1
セキュアコンテナ104を検証
S86－2
セキュアコンテナ104内の各ファイルに
付いて自らの署名データを作成し、当該
署名データとプライエンタデータ等を含む
セキュアコンテナ304を作成してセキュア
コンテナデータベースに格納
S86－3
セキュアコンテナデータベースから
セキュアコンテナ304を読み出してユーザ
ホームネットワークに配給
S86－4
終了

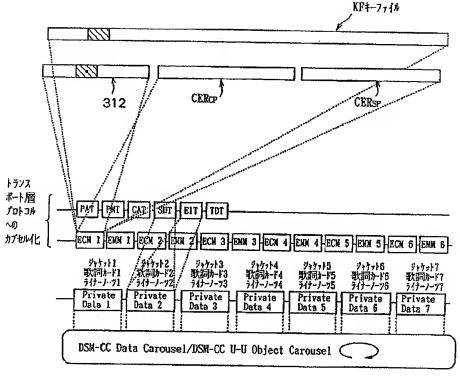
【図８７】


(A)
(B)
(C)
(D)
ヘッダ
コンテンツ鍵データKC
コンテンツデータ
ユーザ特定用データセット
ライセンス鍵データKD1～KDn
SAMプラットフォームカード・コンテナ
プレイコンテンツ(PT)データ
公開鍵証明書
SIG1, ESC
SIG64, SP
SIG1, CP
SIG1, SP

【図８８】


DSD1
CFコンテンツファイル
視聴覚(AV)モジュール
MHEG Content Data
(動画)
MHEG Content Data
(音声)
(静止画)
(テキスト)
(テキスト)
Content
Content -Hook
MHEG Object(動画)
MHEG Object(音声)
MHEG Object(静止画)
MHEG オブジェクトへのカプセル化
MHEGコンテンツデータ
KF
CERSF
ビデオストリップ1
ビデオストリップ2
ビデオストリップ3
ビデオストリップ4
ビデオストリップ5
ビデオストリップ6
ビデオストリップ7
PES-Video 1
PES-Video 2
PES-Video 3
PES-Video 4
PES-Video 6
PES-Video 6
PES-Video 7
トランスポート層プロトコルへのカプセル化
ストリーム1
ストリーム2
ストリーム3
ストリーム4
ストリーム5
ストリーム6
ストリーム7
PES-Audio 1
PES-Audio 2
PES-Audio 3
PES-Audio 4
PES-Audio 6
PES-Audio 6
PES-Audio 7
ジョケット1 歌詞カード1 ライナーノーツ1
ジョケット2 歌詞カード2 ライナーノーツ2
ジョケット3 歌詞カード3 ライナーノーツ3
ジョケット4 歌詞カード4 ライナーノーツ4
ジョケット5 歌詞カード5 ライナーノーツ5
ジョケット6 歌詞カード6 ライナーノーツ6
ジョケット7 歌詞カード7 ライナーノーツ7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

【図８９】



【図９０】

EMDサービスセンタ302の主な機能

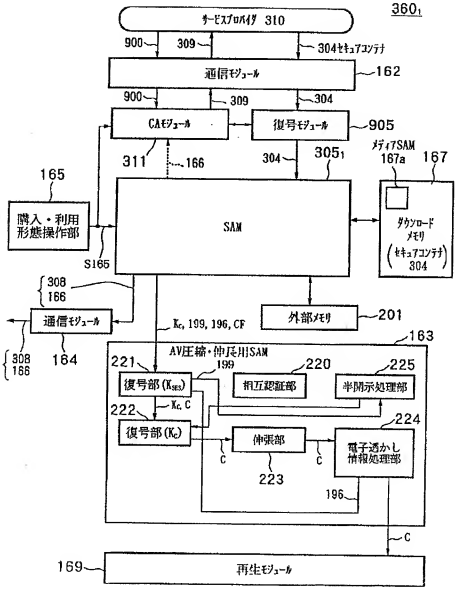
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データDERCP, CERSP, CERSAM1～CERSAMnの発行

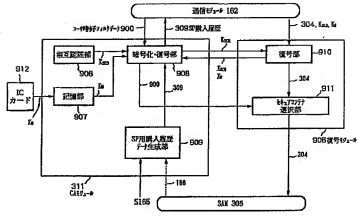
キーファイルKFの生成

利用履歴データに基づき決済処理
(CPとSPとの間の利益分配処理)

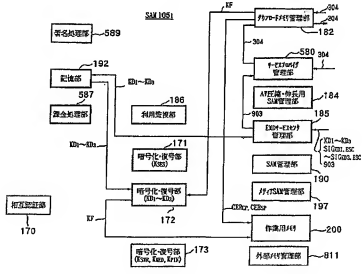
【図９１】


サービスプロバイダ 310
360₁
900
309
304セキュアコンテナ
通信モジュール
162
900
309
304
CAモジュール
復号モジュール
905
311
166
304
305₁
メディアSAM
167a
167
165
購入・利用
形態操作部
SAM
ダウンロード
メモリ
(セキュアコンテナ)
304
S165
308
166
通信モジュール
Kc, 199, 196, CF
外部メモリ
201
163
AV圧縮・伸長用SAM
308
166
164
221
復号部 (KSES)
199
相互認証部
220
半開示処理部
225
222
Kc, C
復号部 (Kc)
伸張部
224
電子透かし
情報処理部
C
C
223
196
C
169
再生モジュール

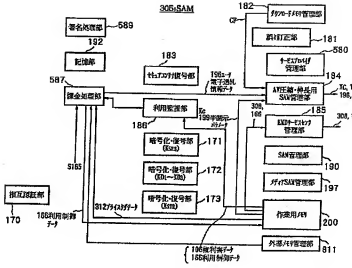
【図９２】


通信モジュール 102
304, Kca, Ks
309 SIM登録入力部
Kca
906
907
908
909
910
911
912
304
Ks
Kca
Ks
Kca
Ks
Ks
304
186
SIM 305

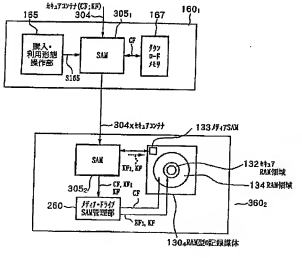
【図９３】


SAM 1051
IF
804
804
182
304
580
304
589
192
587
186
185
984
171
190
197
200
172
170
173
811
903
SIG1, SIG2
304
183
184
KD1～KDn
KD1～KDn
IF
CKDr, CKDp
Kca, Kms, Kry)

【図９５】

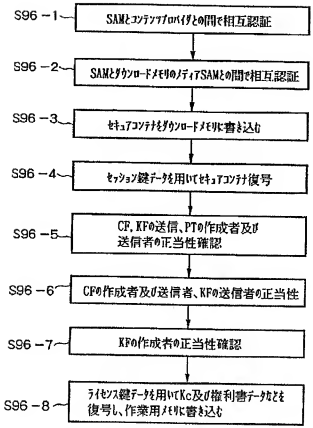

305₁SAM
182
CF
589
192
183
587
181
580
194
185
188
171
172
173
S165
170
200
811
180
197

【図９７】

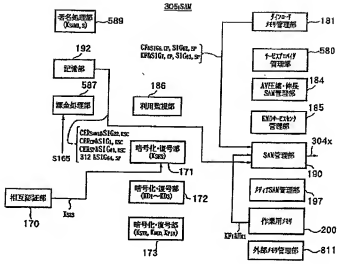

155
304
305₁
157
160₁
SAM
CF
S165
304xｶｰﾄﾞｺﾝﾀｸﾄ
133ﾒﾓﾘSAM
132ｶｰﾄﾞ
134
305₂
260
360₂
130

【図９６】

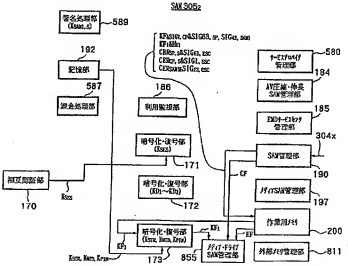
セキュアコンテナの入力処理(SAM)



【図９８】

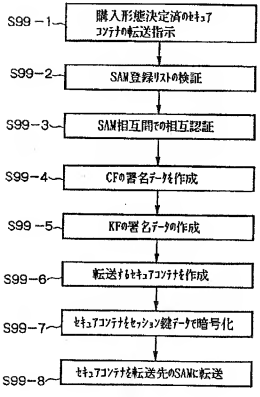

305aSAM
署名処理部 (Xsan, s)
589
192
記憶部
587
資金処理部
186
利用監視部
CERsanSIGn, enc
CERsnSIGn, enc
312 SIGSan, sr
S165
暗号化・復号部 (Xan)
171
相互認証部
Xan
170
暗号化・復号部 (Xbn~Xkn)
172
暗号化・復号部 (Xsn, Xan, Xyn)
173
Xsn, Xan, Xyn
CERsanSIGn, sr, SIGan, sen
KPAsIGn, enSIGSn, sr, SIGan, sen
KPAsIGn
CERsn, nSIGn, enc
CERyn, nSIGn, enc
CERsanSIGn, enc
ﾄﾚｰｻﾋﾞﾘﾃｨ管理部
181
ｲﾝﾃｸﾞﾘﾃｨ管理部
580
ＡＩ圧縮・伸長 SAM管理部
184
ＥＭＩ・ＥＭＣ管理部
185
SAM管理部
304x
190
ﾘｱﾙﾀｲﾑSAM管理部
197
作業用ﾒﾓﾘ
200
KPAsIGn
外部ﾒﾓﾘ管理部
811

【図１０１】

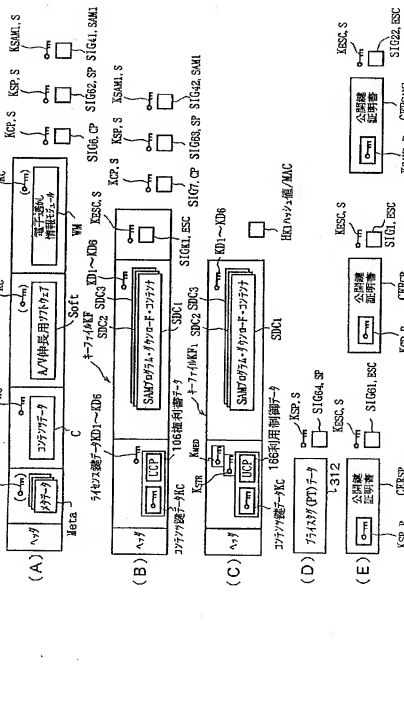

SAM 305z
署名処理部 (Xsan, s)
589
KPAsIGn, enSIGSn, sr, SIGan, sen
KPAsIGn
CERsn, nSIGn, enc
CERyn, nSIGn, enc
CERsanSIGn, enc
192
記憶部
587
資金処理部
186
利用監視部
ﾄﾚｰｻﾋﾞﾘﾃｨ管理部
580
184
ＡＩ圧縮・伸長 SAM管理部
185
ＥＭＩ・ＥＭＣ管理部
304x
暗号化・復号部 (Xan)
171
SAM管理部
190
CF
相互認証部
Xan
170
暗号化・復号部 (Xbn~Xkn)
172
ﾘｱﾙﾀｲﾑSAM管理部
197
暗号化・復号部 (Xsn, Xan, Xyn)
173
KPy
KPy
KPy
作業用ﾒﾓﾘ
200
ﾘｱﾙﾀｲﾑ SAM管理部
855
外部ﾒﾓﾘ管理部
811
Xsn, Xan, Xyn

【図９９】

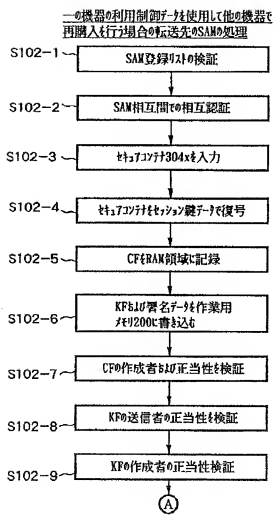
一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送先のSAMの処理



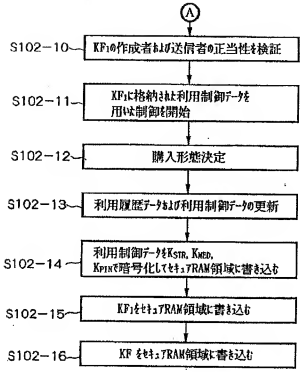
【図１００】


(A) ヘッダ
(B) ヘッダ
(C) ヘッダ
(D) プライバシデータ
(E)
コンテンツ鍵データ用KC
メタデータ
コンテンツデータ
Meta
C
KC
L/V伸長用ソフトウェア
Soft
WM
電子透かし情報埋込み
コンテンツ用MCF
3GAkセキュリティコンテナ
KCP, S
KSAM1, S
S1G6, CP
S1G62, SP
S1G41, SAM1
KSSC, S
KCP, P
CERCP
KSP, S
KSP, P
CERSP
312
S1G64, SP
S1G61, ESC
KSSC, P
CERCP
S1G1, ESC
KSSC, S
KSAM1, P
CERSAM1
S1G22, ESC
ライセンス鍵データ用KD1～KDn
キーファイルKF
SDC2
SDC3
SDC1
SAMアクセス・グループ・コンテクスト
106種利用データ
Kmac
Kstr
S1G41, ESC
KD1～KDn
S1G7, CP
S1G63, SP
S1G42, SAM1
KSAM1, S
KSP, S
KCP, S
KSSC, S
KD1～KDn
キーファイルKF1
SDC2
SDC3
SDC1
SAMアクセス・グループ・コンテクスト
16ビット鍵/MAC
HK1ハッシュ値/MAC
16ビット利用制御データ
KSP, S
S1G64, SP
S1G61, ESC
KSSC, S
KSSC, S
S1G1, ESC
KSAM1, P
CERSAM1
S1G22, ESC

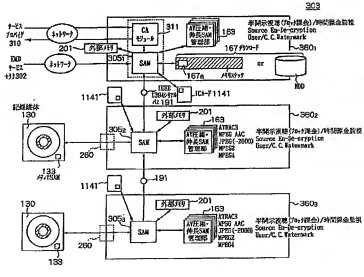
【図１０２】


一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送先のSAMの処理
S102-1
SAM登録リストの検証
S102-2
SAM相互間での相互認証
S102-3
セキュアコンテナ304xを入力
S102-4
セキュアコンテナをセッション鍵データで復号
S102-5
CFをRAM領域に記録
S102-6
KFおよび署名データを作業用メモリ200に書き込む
S102-7
CFの作成者および正当性を検証
S102-8
KFの送信者の正当性を検証
S102-9
KFの作成者の正当性検証
A

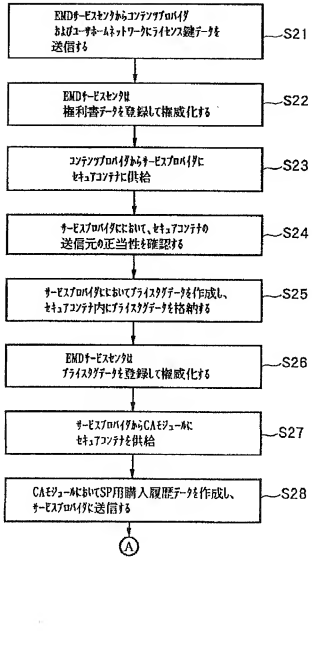
【図１０３】


A
S102－10
KF1の作成者および送信者の正当性を検証
S102－11
XF1に格納された利用制御データを用いた制御を開始
S102－12
購入形態決定
S102－13
利用履歴データおよび利用制御データの更新
S102－14
利用制御データをKSTR, KMED, KPINで暗号化してセキュアRAM領域に書き込む
S102－15
KF1をセキュアRAM領域に書き込む
S102－16
KF をセキュアRAM領域に書き込む

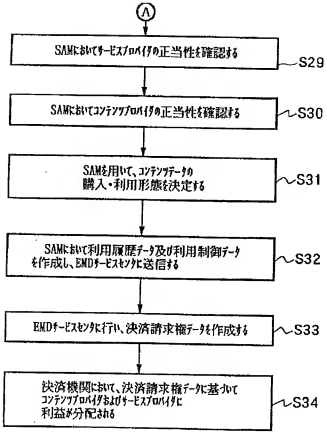
【図１０４】


303
CA セット
311
ATE 端末鍵管理部
153
半導体変換 (アセット組合) /利用額金融機
Source: Re-Encryption
User/C. C. Network
167 バッファ
360a
ROM
ICカードI/F
1141
201
163
ATE 端末鍵管理部
ATRAC3
MPEG AAC
MPEG-2 AAC
MP3
WMA
360b
360c
260
133
130
189
191

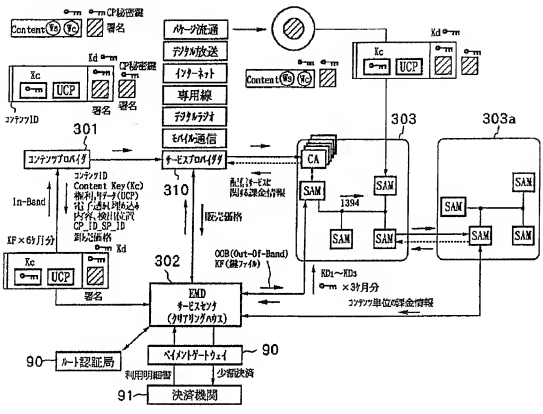
【図１０５】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークにライセンス鍵データを送信する
S21
EMDサービスセンタは権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダにセキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタはプライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールにセキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、サービスプロバイダに送信する
S28
A

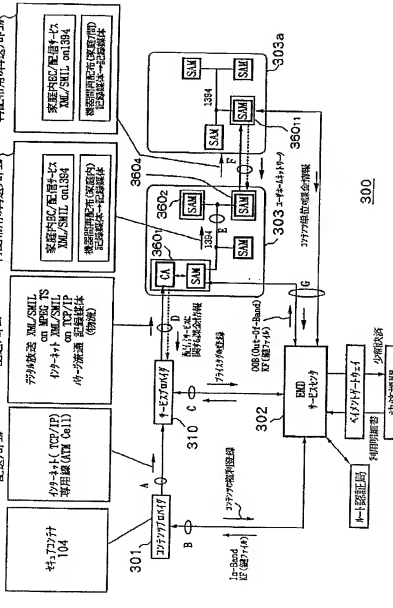
【図１０６】


A
SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの
購入・利用形態を決定する
S31
SAMにおいて利用履歴データ及び利用制御データ
を作成し、EMDサービスセンタに送信する
S32
EMDサービスセンタに行い、決済請求権データを作成する
S33
決済機関において、決済請求権データに基づいて
コンテンツプロバイダおよびサービスプロバイダに
利益が分配される
S34

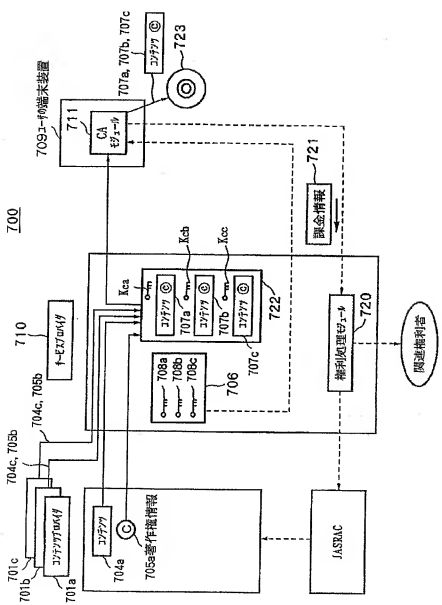
【図１０７】


CP秘密鍵
Content
署名
Kd
Xc
UCP
コンテンツID
301
パケット流通
デジタル放送
インターネット
専用線
デジタルラジオ
モバイル通信
コンテンツプロバイダ
サービスプロバイダ
310
303
303a
CA
SAM
1394
In-Band
コンテンツID
Content Key(Kc)
権利データ(UCP)
XF（ファイル）
内容、検出記号
CP_ID_SP_ID
割当価格
KF×6ヶ月分
販売価格
302
OOB(Out-Of-Band)
KF(鍵ファイル)
KD1～KD3
×3ヶ月分
コンテンツ単位の課金情報
EMD
サービスセンタ
(クリアリングハウス)
90
カード認証局
ペイメントゲートウェイ
利用明細書
少額決済
91
決済機関

[図１０８]


家庭内配信/機器間再配布用の暗号方式
家庭内配信/配信サービス XML/SMIL on1394
機器間再配布(家庭内)記録媒体→記録媒体
家庭内配信/機器間再配布用の暗号方式
家庭内配信/配信サービス XML/SMIL on1394
機器間再配布(家庭内)記録媒体→記録媒体
チューナ/ケータイ用配送方式
デジタル放送 XML/SMIL on MPEG TS
インターネット XML/SMIL on TCP/IP
パーソナル通信 記録媒体(物理)
コアネットワーク用配送方式
インターネット(TCP/IP)専用線(ATM Cell)
セキュアコンテナ104
301
コアネットワークIFA
A
B
310
c
チューナIF
D
Ad-hoc/IrDA/赤外線
コアネットワーク制御線
1394/USB2.0(赤外線)
アクセス制御線
302
IEEE1394 チューナ
OOB(Out-Of-Band)(赤外線)
コアネットワーク制御情報
G
303
コンテンツ蓄積メカニズム
303a
360a
360b
360c
360d
360e
360f
360g
360h
360i
360j
360k
360l
360m
360n
360o
360p
360q
360r
360s
360t
360u
360v
360w
360x
360y
360z
360aa
360ab
360ac
360ad
360ae
360af
360ag
360ah
360ai
360aj
360ak
360al
360am
360an
360ao
360ap
360aq
360ar
360as
360at
360au
360av
360aw
360ax
360ay
360az
360ba
360bb
360bc
360bd
360be
360bf
360bg
360bh
360bi
360bj
360bk
360bl
360bm
360bn
360bo
360bp
360bq
360br
360bs
360bt
360bu
360bv
360bw
360bx
360by
360bz
360ca
360cb
360cc
360cd
360ce
360cf
360cg
360ch
360ci
360cj
360ck
360cl
360cm
360cn
360co
360cp
360cq
360cr
360cs
360ct
360cu
360cv
360cw
360cx
360cy
360cz
360da
360db
360dc
360dd
360de
360df
360dg
360dh
360di
360dj
360dk
360dl
360dm
360dn
360do
360dp
360dq
360dr
360ds
360dt
360du
360dv
360dw
360dx
360dy
360dz
360ea
360eb
360ec
360ed
360ee
360ef
360eg
360eh
360ei
360ej
360ek
360el
360em
360en
360eo
360ep
360eq
360er
360es
360et
360eu
360ev
360ew
360ex
360ey
360ez
360fa
360fb
360fc
360fd
360fe
360ff
360fg
360fh
360fi
360fj
360fk
360fl
360fm
360fn
360fo
360fp
360fq
360fr
360fs
360ft
360fu
360fv
360fw
360fx
360fy
360fz
360ga
360gb
360gc
360gd
360ge
360gf
360gg
360gh
360gi
360gj
360gk
360gl
360gm
360gn
360go
360gp
360gq
360gr
360gs
360gt
360gu
360gv
360gw
360gx
360gy
360gz
360ha
360hb
360hc
360hd
360he
360hf
360hg
360hh
360hi
360hj
360hk
360hl
360hm
360hn
360ho
360hp
360hq
360hr
360hs
360ht
360hu
360hv
360hw
360hx
360hy
360hz
360ia
360ib
360ic
360id
360ie
360if
360ig
360ih
360ii
360ij
360ik
360il
360im
360in
360io
360ip
360iq
360ir
360is
360it
360iu
360iv
360iw
360ix
360iy
360iz
360ja
360jb
360jc
360jd
360je
360jf
360jg
360jh
360ji
360jj
360jk
360jl
360jm
360jn
360jo
360jp
360jq
360jr
360js
360jt
360ju
360jv
360jw
360jx
360jy
360jz
360ka
360kb
360kc
360kd
360ke
360kf
360kg
360kh
360ki
360kj
360kk
360kl
360km
360kn
360ko
360kp
360kq
360kr
360ks
360kt
360ku
360kv
360kw
360kx
360ky
360kz
360la
360lb
360lc
360ld
360le
360lf
360lg
360lh
360li
360lj
360lk
360ll
360lm
360ln
360lo
360lp
360lq
360lr
360ls
360lt
360lu
360lv
360lw
360lx
360ly
360lz
360ma
360mb
360mc
360md
360me
360mf
360mg
360mh
360mi
360mj
360mk
360ml
360mm
360mn
360mo
360mp
360mq
360mr
360ms
360mt
360mu
360mv
360mw
360mx
360my
360mz
360na
360nb
360nc
360nd
360ne
360nf
360ng
360nh
360ni
360nj
360nk
360nl
360nm
360nn
360no
360np
360nq
360nr
360ns
360nt
360nu
360nv
360nw
360nx
360ny
360nz
360oa
360ob
360oc
360od
360oe
360of
360og
360oh
360oi
360oj
360ok
360ol
360om
360on
360oo
360op
360oq
360or
360os
360ot
360ou
360ov
360ow
360ox
360oy
360oz
360pa
360pb
360pc
360pd
360pe
360pf
360pg
360ph
360pi
360pj
360pk
360pl
360pm
360pn
360po
360pp
360pq
360pr
360ps
360pt
360pu
360pv
360pw
360px
360py
360pz
360qa
360qb
360qc
360qd
360qe
360qf
360qg
360qh
360qi
360qj
360qk
360ql
360qm
360qn
360qo
360qp
360qq
360qr
360qs
360qt
360qu
360qv
360qw
360qx
360qy
360qz
360ra
360rb
360rc
360rd
360re
360rf
360rg
360rh
360ri
360rj
360rk
360rl
360rm
360rn
360ro
360rp
360rq
360rr
360rs
360rt
360ru
360rv
360rw
360rx
360ry
360rz
360sa
360sb
360sc
360sd
360se
360sf
360sg
360sh
360si
360sj
360sk
360sl
360sm
360sn
360so
360sp
360sq
360sr
360ss
360st
360su
360sv
360sw
360sx
360sy
360sz
360ta
360tb
360tc
360td
360te
360tf
360tg
360th
360ti
360tj
360tk
360tl
360tm
360tn
360to
360tp
360tq
360tr
360ts
360tt
360tu
360tv
360tw
360tx
360ty
360tz
360ua
360ub
360uc
360ud
360ue
360uf
360ug
360uh
360ui
360uj
360uk
360ul
360um
360un
360uo
360up
360uq
360ur
360us
360ut
360uu
360uv
360uw
360ux
360uy
360uz
360va
360vb
360vc
360vd
360ve
360vf
360vg
360vh
360vi
360vj
360vk
360vl
360vm
360vn
360vo
360vp
360vq
360vr
360vs
360vt
360vu
360vv
360vw
360vx
360vy
360vz
360wa
360wb
360wc
360wd
360we
360wf
360wg
360wh
360wi
360wj
360wk
360wl
360wm
360wn
360wo
360wp
360wq
360wr
360ws
360wt
360wu
360wv
360ww
360wx
360wy
360wz
360xa
360xb
360xc
360xd
360xe
360xf
360xg
360xh
360xi
360xj
360xk
360xl
360xm
360xn
360xo
360xp
360xq
360xr
360xs
360xt
360xu
360xv
360xw
360xx
360xy
360xz
360ya
360yb
360yc
360yd
360ye
360yf
360yg
360yh
360yi
360yj
360yk
360yl
360ym
360yn
360yo
360yp
360yq
360yr
360ys
360yt
360yu
360yv
360yw
360yx
360yy
360yz
360za
360zb
360zc
360zd
360ze
360zf
360zg
360zh
360zi
360zj
360zk
360zl
360zm
360zn
360zo
360zp
360zq
360zr
360zs
360zt
360zu
360zv
360zw
360zx
360zy
360zz
SAM
1394
E
F
300
ネットワーク
利用制御部
決済機関
決済機関

【図１０９】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
H04N 7/173	640	H04N 7/167	Z

Ｆターム(参考) 5B085 AC04 AE02 AE03 AE04 AE09
AE29
5C064 BA01 BB01 BB07 BC01 BC17
BC22 BD02 BD04 BD08
5J104 AA01 AA07 AA09 AA14 AA16
AA45 AA46 EA17 KA01 KA07
LA03 LA06 NA02 NA03 NA42
PA07 PA10 PA11
9A001 JJ19 JJ67 LL03

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成18年5月11日(2006.5.11)

【公開番号】特開2001-175605(P2001-175605A)
【公開日】平成13年6月29日(2001.6.29)
【出願番号】特願平11-359896
【国際特許分類】
Ｇ０６Ｆ　21/00　(2006.01)
Ｈ０４Ｈ　1/00　(2006.01)
Ｈ０４Ｎ　7/173　(2006.01)
Ｇ１０Ｌ　11/00　(2006.01)
Ｈ０４Ｌ　9/10　(2006.01)
Ｈ０４Ｎ　7/167　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｈ０４Ｈ　1/00　Ｆ
Ｈ０４Ｎ　7/173　６４０Ａ
Ｇ１０Ｌ　9/00　Ｅ
Ｈ０４Ｌ　9/00　６２１Ａ
Ｈ０４Ｎ　7/167　Ｚ

【手続補正書】
【提出日】平成18年3月17日(2006.3.17)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを入力する処理を行う入力処理手段と、
前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、
前記決定の結果を示す履歴データを生成する履歴データ生成手段と、
前記コンテンツ鍵データを復号する復号手段と
を耐タンパ性の回路モジュール内に有する
データ処理装置。
【請求項２】
前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成する利用制御データ生成手段と、
前記利用制御データに基づいて、前記コンテンツデータの利用を制御する利用制御手段と
を前記耐タンパ性の回路モジュール内にさらに有する
請求項１に記載のデータ処理装置。
【請求項３】
前記入力処理手段は、前記コンテンツ鍵データおよび前記権利書データの署名データを入力する処理をさらに行い、

前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項４】
前記入力処理手段は、前記コンテンツデータの署名データを入力する処理をさらに行い、
前記データ処理装置は、
前記署名データの正当性を検証する署名処理手段
を耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項５】
前記入力処理手段は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて秘密鍵データを用いて作成された署名データと、前記秘密鍵データに対応する公開鍵データとを入力する処理をさらに行い、
前記データ処理装置は、
前記公開鍵データを用いて、前記署名データの正当性を検証する署名処理手段を前記耐タンパ性の回路モジュール内にさらに有し、
前記決定手段は、前記署名処理手段によって前記署名データの正当性が確認された後に、前記決定を行う
請求項１に記載のデータ処理装置。
【請求項６】
前記コンテンツ鍵データは、ライセンス鍵データを用いて暗号化されており、
前記データ処理装置は、
前記ライセンス鍵データを記憶する記憶手段
をさらに有し、
前記復号手段は、前記記憶手段から読み出した前記ライセンス鍵データを用いて前記コンテンツ鍵データを復号する
請求項１に記載のデータ処理装置。
【請求項７】
前記データ処理装置は、他の装置との間で、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一のデータをオンラインで送受信する場合に、前記他の装置との間で相互認証を行う相互認証手段と、
前記相互認証によって得られたセッション鍵データを用いて、前記送受信を行うデータの暗号化および復号を行う暗号化・復号手段と
を前記耐タンパ性の回路モジュール内にさらに有する
請求項１に記載のデータ処理装置。
【請求項８】
コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置において、
当該データ処理装置の秘密鍵データを記憶する記憶回路と、
前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、

前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、

前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項９】

コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、

他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、

前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項１０】

ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、

他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、

他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、

前記相互認証を行うために乱数を生成する乱数生成回路と、

演算処理回路と、

前記記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】００１４

【補正方法】削除

【補正の内容】

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】００１６

【補正方法】削除

【補正の内容】

【手続補正４】

【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】削除
【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】削除
【補正の内容】
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】削除
【補正の内容】
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】削除
【補正の内容】
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】削除
【補正の内容】
【手続補正１４】

【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】削除
【補正の内容】
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】削除
【補正の内容】
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】削除
【補正の内容】
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】削除
【補正の内容】
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】削除
【補正の内容】
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００３２
【補正方法】変更
【補正の内容】
【００３２】
本発明のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化されたコンテンツ鍵データを復号するデータ処理装置であって、当該データ処理装置の秘密鍵データを記憶する記憶回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成する公開鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成する乱数生成回路と、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する共通鍵暗号回路と、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路との間のデータ転送を外部バスを介して行う外部バスインターフェイスと、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する演算処理回路とを耐タンパ性の回路モジュール内に有する。
【手続補正２０】

【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】削除
【補正の内容】
【手続補正２１】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】削除
【補正の内容】
【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】削除
【補正の内容】
【手続補正２３】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】削除
【補正の内容】
【手続補正２５】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正２６】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正２７】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】
【手続補正２８】
【補正対象書類名】明細書
【補正対象項目名】００４１
【補正方法】削除
【補正の内容】
【手続補正２９】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】削除
【補正の内容】
【手続補正３０】

【補正対象書類名】明細書
【補正対象項目名】００４３
【補正方法】削除
【補正の内容】
【手続補正３１】
【補正対象書類名】明細書
【補正対象項目名】００４４
【補正方法】削除
【補正の内容】
【手続補正３２】
【補正対象書類名】明細書
【補正対象項目名】００４５
【補正方法】削除
【補正の内容】
【手続補正３３】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】削除
【補正の内容】
【手続補正３４】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】変更
【補正の内容】
【００４７】
また、本発明のデータ処理装置は、コンテンツデータの圧縮および伸長のうち少なくとも一方を行うデータ処理装置であって、他の装置との間で相互認証を行い、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、データの圧縮および伸長の少なくとも一方を行う圧縮・伸長回路と、前記圧縮および伸長の対象となるデータに対して電子透かし情報の検出および埋め込みを行う電子透かし情報処理回路とを耐タンパ性の回路モジュール内に有する。
【手続補正３５】
【補正対象書類名】明細書
【補正対象項目名】００４８
【補正方法】削除
【補正の内容】
【手続補正３６】
【補正対象書類名】明細書
【補正対象項目名】００４９
【補正方法】変更
【補正の内容】
【００４９】
また、本発明のデータ処理装置は、ＲＯＭ型またはＲＡＭ型の記録媒体にアクセスを行うデータ処理装置であって、他の装置との間で入出力されるデータのハッシュ値を生成するハッシュ値生成回路と、他の装置との間で相互認証を行い、他の装置が作成した署名データを共通鍵データおよび前記ハッシュ値を用いて検証し、前記ハッシュ値および前記共通鍵データを用いて署名データを作成し、他の装置との間で入出力するデータを、前記相互認証によって得られたセッション鍵データを用いて暗号化および復号する共通鍵暗号回路と、前記相互認証を行うために乱数を生成する乱数生成回路と、演算処理回路と、前記

記録媒体に記録するデータをエンコードし、前記記録媒体から読み出したデータをデコードするエンコード・デコード回路とを耐タンパ性の回路モジュール内に有する。
【手続補正３７】
【補正対象書類名】明細書
【補正対象項目名】００５０
【補正方法】削除
【補正の内容】
【手続補正３８】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】削除
【補正の内容】
【手続補正３９】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】削除
【補正の内容】
【手続補正４０】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】削除
【補正の内容】